An Arbitrator's Perspective: Confidentiality – Privacy – Security in the Eye of the Arbitrators or the Story of the Arbitrator who Became a Bee

Marc Henry

My subject is: how shall the questions of confidentiality, privacy and security be addressed by the arbitrator in an online arbitration? And do these imperatives represent new challenges for the arbitrators when they are applied to online arbitration?

An alternative title for this article might be "The Bee and the Arbitrator".

To start with a preliminary observation: in this article, the notion of ODR and therefore of Online Arbitration will have the meaning given by UNCITRAL in its 2017 Technical Notes on Online Dispute Resolution. In section V of the Notes, online dispute resolution is defined as: 'a mechanism for resolving disputes through the use of electronic communications and other information and communication technology'. So it turns out that we have been practising online arbitration for a long time: indeed, it is sufficient that electronic means of communication are used in the arbitration procedure for the procedure to be considered an ODR. Email is an electronic means of communication. If the participants in an arbitral procedure communicate by email, the arbitration will therefore fall within the concept of ODR. This means that arbitration procedures have already been hybrid for a long time, using both online and offline dispute resolution processes.

While the use of the Internet in arbitration is now common, it should be remembered that just 20 years ago, as reported by one author[1], ICCA President (Fari Nariman), at the ICCA annual conference in Washington on November 10, 2000, expressed great scepticism about the importance the impersonal world of the Internet might attain in the intensely personal

1 Alford, 'The Virtual World and the Arbitration World' (2001) 18-4 *Journal of International Arbitration*, 449.

world of international arbitration. What is more, in its Report on Information Technology in International Arbitration of 2017, the ICC states that when the task force issued its 2004 report, some anecdotes from arbitration practitioners suggested that there were arbitrators who refused to communicate by email or at least were reluctant to do so (page 21 of the report). Today, communication via email and other electronic means has become standard practice for nearly all parties and arbitrators (*ibid*).

So, Fari Nariman was wrong. After 9-11, and the pandemic, the Internet has indeed revolutionised arbitration. But to what extent? If emails have become the normal means of communication in arbitration proceedings, we can observe that videoconferencing has only recently appeared in arbitrations[2]. However, this technology had already existed for a long time. Skype or Facetime had long been used to organize virtual meetings. Back in 2017, as one author notes, the ICC observed that 'many widely available information Technology (IT) solutions are not used to save time and costs as effectively as they could be. For instance, parties and tribunals were reluctant to use videoconferencing even for minor witnesses, when such solution could easily cut time and costs' [3].

Similarly, ODRs and especially online arbitration seemed to be reserved for the resolution of small commercial and consumer disputes in e-commerce[4]. We have seen Amazon or Ebay include ODRs in their general terms of sale. However, the resolution of major international disputes has remained resistant to the use of video. In 2001, an author observed that: 'In the international context, it is quite common for hearings to last for several days. It seems unlikely that parties and arbitrators would happily discourse in private examinations and informal caucus sessions that are critical to such hearings'[5].

Finally, the use of information technology in arbitration has occurred where it was not expected: in international arbitration. But a catalyst was needed for this: this catalyst happened to be COVID and the impossibility of in-person hearings. The first reflex of arbitration actors was to postpone

2 On the topic, see ICC, *ICC Commission Report, Information Technology in International Arbitration*, 2017.

3 Goh, 'Digital Readiness Index for Arbitration Institutions: Challenges and Implications for Dispute Resolution under the Belt and Road Initiative' (2021) 38-2 *Journal of International Arbitration*, 253; ICC, *ICC Commission Report, Information Technology in International Arbitration*, 2017.

4 Alford, 'The Virtual World and the Arbitration World' (2001) 18-4 *Journal of International Arbitration*, 449.

5 Ibid.

the hearings. Then, in a second phase, faced with the unforeseeability of when normality might return, the actors had to resolve to organise virtual hearings.

Paradoxically, therefore, ODR has not been developed in judicial litigation, where it would seem to be very appropriate, given that judges have little or almost no more time to listen to the pleadings of lawyers and that if pleadings are eliminated, ODR becomes the most effective means of settling disputes. Instead, ODR has expanded into an area where hearings still play a major role, namely international commercial arbitration.

In short, what has really changed in recent times in online arbitrations is, in addition to the electronic exchange of documents, the use of virtual hearings.

Therefore, to assess the existence of new challenges in the use of Online Arbitrations today, and so to answer the question posed in the conference, it will be necessary to consider whether the increasingly frequent use of virtual hearings creates new challenges with regard to the imperatives of confidentiality, privacy and security for arbitrators.

One question immediately presents itself: why should Online Arbitrations create challenges *now*, and maybe even *new* challenges for arbitrators, in terms of confidentiality, privacy and security? The answer can be found in two words: "data" and "online".

As soon as exchanges and hearings are no longer carried out by physical means (mail, courtroom) but rather electronically (email, virtual hearings), the data forming the subject of the exchanges and hearings moves out of the physical domain and into cyberspace. This line of development is unsurprising. The fields in which human conflict is played out have evolved as human technology has progressed. To land, we have added the sea, the air, outer space and now a fifth field of conflict: cyberspace. In fact, rather than space, the idea of a universe might better evoke internet and the volume of digital data created. The volume generated annually has increased twenty-fold in ten years.

In 2018, the annual volume was 33 zettabytes of data: this represents the storage capacity of 660 billion Blue Rays or ... 33 million human brains. By 2020 we were talking about 50 zettabytes. And a zettabyte is a trillion bytes and a trillion bytes is a thousand billion bytes: a 1 followed by 21 zeros. This is what the annual volume of digital data creation represents.

The scale of the universe of digital data therefore rivals the scale of astrophysics, and even exceeds it. Speaking about perception of scales, Darwin wrote that: 'The mind cannot possibly grasp the full meaning of the term of one hundred million years'. So, one can imagine how difficult it can be to conceive of scales measured in trillions!

The difficulty of grasping the universe of digital data explains the difficulty that we all have, including arbitrators, course, in apprehending this universe, and so in perceiving and responding to the growing threats in this new dimension of human activity. The response to cyber threats is made all the more difficult by the absence of frontiers in cyberspace. It has been designed to free itself from borders, to do away with territories. Attempts to combat hackers can therefore look like trying to catch a chicken in open country.

We fail to realise that when we send an email, or when we hold a virtual hearing, it is like sending a post card. The content of the email or the video, like the content of a postcard, can be seen by third parties: Post Office staff in the case of postcards, the IT administrator of the company or the internet service provider in the case of emails or videos. The idea of a postcard is a good way for arbitrators visualise and be aware of the risks entailed by sending data into cyberspace.

Not only is email a postcard, but its use is much riskier because, unlike a card, it is so easy to send an email or a file to the wrong recipient[6].

Despite these risks, many arbitrators still do not fully realize what data is exposed to in an arbitration.

By feeding cyberspace with the data forming the subject matter of an arbitration, the arbitration players expose themselves to a much greater risk of third parties becoming aware of, capturing or even misappropriating this data.

This threat is not imaginary. There is the example of the attack against the website of the Permanent Court of Arbitration of the Hague at the time of the *China v. Philippines* arbitration in 2015 using the water hole technique. Just recently, in March/April 2021, allegations of a cyber-attack on a Brazilian multi-billion-dollar arbitration called into question the award rendered by the arbitral tribunal.

But then, in this context, is the arbitrator condemned, like Pessoa, to make unrest a constant feature of his activity? Certainly not.

Why? Precisely because confidentiality, privacy and security are instruments designed to avoid this kind of stress.

To illustrate my reasoning – and having just evoked Pessoa - I feel obliged to use a metaphor. The activity of the arbitrator, the space he creates when he joins an arbitral tribunal, is often described as a "black box". For my part, to draw this time on an animal metaphor, I will compare

6 See ICC, *ICC Commission Report, Information Technology in International Arbitration*, 2017, 15.

this space, and more generally the arbitration institution, to a beehive, in which the arbitrators are both the worker bees and the soldier bees. In these arbitral hives, the pollen will represent the digital data brought into the arbitrations, the honey representing the ultimate work of the arbitrator bee, i.e. the awards!

Like a bee in a hive, the arbitrator takes on two roles: those of both worker and soldier.

Confidentiality and privacy pertain to the role of worker arbitrator, while security pertains to the role of soldier arbitrator. These two aspects of the arbitrator's mission will be covered below.

A. The Contribution of Worker Arbitrators to Confidentiality and Privacy in the Arbitral Hives

Worker bees have the dual task of storing pollen and processing it to make honey. As such, they are both receivers and processors of pollen.

Similarly, in their arbitral hives, the worker arbitrators are both receivers and processors of a high-density pollen: the digital data. These digital data is the indispensable material for creating the finished product, the award, just as pollen is the necessary raw material for confecting honey.

The purpose of confidentiality is to keep the data at the disposal of the persons authorised to have access to the data. Confidentiality therefore relates to the data storage activity of the worker arbitrators in their arbitral hives. The purpose of privacy is to ensure fair and authorised processing of personal data. Privacy therefore relates to the data processing activity of the worker arbitrators in their arbitral hives.

I will study these two imperatives in the worker arbitrators activity successively.

I. Confidentiality in the Arbitrator's Data Storage Activity

What does confidentiality mean? Confidentiality is preventing unauthorised access to digital data to non-public information that two or more parties have agreed to restrict. Confidential is an imposed label that signifies access control. In other words, confidentiality applies to data and serves to define who can have access to the data and how the data may be used by those who have access.

When arbitration was entirely organised in physical form, when letters were exchanged by post, when the terms of reference were signed during a meeting to launch the procedure, when hearings were held in person, it was obvious that arbitration was understood to be a strictly confidential form of justice, unlike state justice.

The title of the conference reflects this mindset. The requirement of confidentiality in arbitration is asserted as a given. However, this confidentiality, or at least its absolute character, has been questioned for some years.

It seems that this challenge dates from the advent of the internet. My analysis is that the use of the internet and the digitisation of exchanges and data that it brings, imbues its users with an unconscious propensity for transparency. This may be due to the feeling that in cyberspace, it is futile to believe that data can remain confidential and that the best thing would be to abandon any idea of confidentiality or at least to reduce its scope as soon as the arbitration takes place in cyberspace.

- Since confidentiality is no longer a constant in arbitration (in French law, it is *de jure* in domestic arbitration according to article 1464 of the Code of Civil Procedure, but it is no longer automatic in international arbitration, even if French case law continues to consider it as a principle applicable in this field), it is necessary to certify whether it is required. This is particularly true in the case of online arbitration. Several scenarios are possible:
- The parties have provided in the arbitration agreement for a seat of arbitration (which is assumed to be virtual): this seat makes it possible to determine a *lex arbitri* which may or may not be the basis for the confidentiality requirement,
- The parties have established the confidentiality requirement in the arbitration agreement, or an obligation to this effect is provided for in the arbitration rules applicable in the event of recourse to institutional arbitration (we may recall that the ICC Arbitration Rules no longer institute a confidentiality principle): in the event of online arbitration, the arbitrators will of course have to observe and ensure observance of this requirement,
- The parties have not provided for an arbitration seat in the arbitration agreement and a confidentiality requirement is not included in either the arbitration agreement or the arbitration rules: in this event, if the parties disagree, the question will arise for the arbitrator as to whether such a requirement must be respected: in the absence of a designated seat of arbitration, the arbitrator will not be able to find an answer

in the *lex arbitri* that could be designated in the light of such seat; moreover, the use of online arbitration may be interpreted as the parties' will to exclude the application of any *lex arbitri* to the arbitration. How should we then answer the question of whether or not there is a confidentiality requirement in an online arbitration? It seems to me that, notwithstanding the reticence expressed by some authors (but not by companies) on the appropriateness of a confidentiality principle in international arbitration, the reason why companies resort to arbitration continues to be the confidentiality it offers and that this requirement therefore constitutes a transnational arbitration principle that the arbitrator should apply and enforce, even in an online arbitration.

We will therefore assume that the principle of confidentiality is maintained. The worker arbitrator will have to make sure that:

- this principle is well noted by the parties,
- that the necessary steps are taken to ensure that the data is stored in such a way that this confidentiality is guaranteed, and
- that only authorised persons can have access to this data.

The arbitrator should insist that counsel and the parties remind all persons with access to the digital data that the data is strictly confidential and should not be transferred without the express consent of the person from whom it originated. The arbitrator must also ensure that his or her assistant and any secretary to the arbitral tribunal scrupulously respects the confidentiality of the data and does not disseminate it to any unauthorized person. If the arbitrator is a lawyer in a law firm, he or she shall ensure that access to the data is not freely available in the law firm.

To this end, lawyers acting for parties must include a confidentiality clause in the arbitration clause and arbitrators must include one in the Terms of Reference. And this needs to be done even if the applicable arbitration rules or the applicable *lex arbitri* provide for such confidentiality.

In addition to the commitments by the actors in the arbitration procedure that the arbitrator should obtain, there is a technical means to facilitate compliance with confidentiality. This is the use of digital Platforms. As noted by practicians in a recent report published in July 2020 by a working group on LegalTech Adoption in International Arbitration, these Platforms can enable administrators to control access to specific folders/data and generate alert/audit trails if data is shared with anyone lacking the necessary access permissions. Platforms can also enable administrators to grant partial access permissions to data so that certain individuals or

groups can view particular documents but not edit, send or print them[7]. Encryption methods can also enhance confidentiality since they protect against information leakage.

Finally, because virtual hearings dramatically expanded during the COVID outbreak, many practitioners now urge arbitrators to invite the arbitral actors to conclude Protocols defining the terms for these remote hearings[8], i.e.:

- The technology used must allow all participants to feel secure about the confidentiality of the information disclosed in the remote hearing,
- Access to the virtual hearing rooms and breakout rooms to be strictly limited to their allocated participants,
- Full names and roles of all participants in a remote hearing, including counsel, parties, witnesses, interpreters, tribunal secretaries and computer technicians, as well as their allocated virtual hearing and breakout rooms, to be circulated in advance and strictly adhered to,
- Physical rooms occupied by participants in remote proceedings, either in their homes, offices, or in special hearing venues, to be separate from non-participants in the remote proceedings, soundproofed where possible, and offering sufficient visibility to eliminate the possibility of undisclosed non-participating individuals, and/or any video recording equipment that has not been agreed to, being present in the room.

That said, from my personal perspective as an arbitrator, I must confess that I have only once recommended the use of such Protocol, in view of the sensitivity of the subject matter.

The protection of confidentiality in online arbitrations is all the more essential if we consider that digitisation of arbitration data leads the institutions supervising them to wish to process this data, in particular the awards, in order to make it public. The best example is the ICC which, as a matter of principle and save as otherwise expressly requested by the parties, has been publishing on its website, since 2016: the names of the arbitrators, their nationality, their role within the tribunals, details of their appointment and whether the arbitration has been closed or concluded. In addition, awards and/or orders, as well as dissenting opinions issued since 1 January 2019, have been subject to publication under certain conditions.

---

7 Working Group on LegalTech Adoption in International Arbitration, *Protocol for Online Case Management in International Arbitration*, July 2020.

8 See for instance, CIArb, *Guidance Note on Remote Dispute Resolution Proceedings*, 2020, 5.

It is therefore clear that confidentiality is a principle whose scope is being reduced, surprisingly on the initiative of certain major players in arbitration. I believe that a growing trend in this direction would be dangerous for arbitration, for several reasons.

- Firstly, arbitration is not state justice. The imperatives of transparency and publication of case law imposed on state justice are not intended, in principle, to be transposed to arbitration.
- Secondly, publication is not what arbitration users, i.e. companies, are looking for. They want confidentiality, and it is surprising to note that some actors who derive their livelihood from arbitration seem to ignore this fundamental wish of the users. Dogmatism is not a positive value in arbitration.

In view of the increasing digitisation of arbitration, whether in terms of data, means of communication, or hearings, to undermine the principle of confidentiality seems to me to create an environment where a less severe line is taken on the hacking and/or undue disclosure of data that is, in principle, confidential and that is transmitted and exchanged in arbitrations. This can only be detrimental to the institution.

I have previously had the opportunity to denounce this risk in an article published in 2019[9]. To devalue the principle of confidentiality in arbitration necessarily means reducing its scope and consequently exposing arbitrators to the risk of reducing the scope of the professional secrecy that they could enforce against public authorities seeking to seize the arbitration data in their possession. In fully digitized arbitration proceedings, it will be much easier for public authorities to seize the entirety of the data in the possession of one of the participants in the arbitration, and of the arbitrator in particular. And what is certain is that the risk of such seizure will increase in the years ahead: either because arbitration constitutes the actual instrument of a criminal offence, or because arbitration is more and more subject to circumstances likely to constitute a criminal offence. As I concluded in my article, arbitration proceedings, and online arbitrations in particular, should not become the antechamber of the public prosecutor's office[10].

- Lastly, in France at least, an Act of 23 March 2019 established a general framework regulating online arbitration platforms by providing

9 M. Henry, 'Infraction pénale et confidentialité de l'arbitrage : devoirs et obligations des arbitres et des conseils' (2019) 1 *Revue de l'Arbitrage*, 65.

10 *Ibid*.

> for a certification procedure and a certain number of conditions for benefiting from it. Under French law, these platforms are subject to three essential obligations: respect for the protection of personal data (we will come back to this), pursuit of their mission with impartiality, independence, competence and diligence, and the obligation of confidentiality (unless otherwise agreed by the parties). Breach of this last obligation is a criminal offence (Article 226-13 of the Penal Code). This means that, for the legislator at least, confidentiality rightly still lies at the heart of arbitration, and in particular of online arbitration[11].

An arbitrator who breaches confidentiality may be liable to a party to the arbitration if the breach is prejudicial. Such a breach would not be committed in the exercise of his or her adjudicative function *per se.* It should therefore not be covered by the immunity that arbitrators enjoy in the exercise of their jurisdictional function. The obligation of confidentiality is part of the arbitrator's contract with the parties. The breach of this obligation constitutes a contractual fault for which the arbitrator must in principle compensate. However, it has been observed how easy it can be in an online arbitration to make a data handling mistake (in particular, the transmission of an email to the wrong person). This makes it even easier to violate the confidentiality obligation.

Therefore, I cannot sufficiently stress the need for arbitrators to include a disclaimer in the arbitration rules of the institutions or in the Terms of Reference. Under French law, only particularly serious and inexcusable that faults could allow such a clause to be set aside.

There is one last question that concerns the storage of pollen data by the worker arbitrators. It is the risk of the beehive taking in pollen that may be compromised. I mean by this the risk of admitting into the arbitration data originating from a cyberattack. This issue will probably occur more and more frequently. How should this data be treated by the worker arbitrators in their arbitral hives? Should the arbitrators disallow the admission of this data in the arbitration because of its fraudulent origin? Or should the arbitrators accept the data if it happens to be essential to an understanding of the issues at stake? These two solutions have already been adopted in arbitral case law (against admission in the *ConocoPhilips v/ Venezuela* case and in favour of admission in the *Caratube International v/ Kazakhstan* case). Article 9-2 of the IBA Rules on the Taking of evidence in International Arbitration permits arbitrators to exclude evidence on

11 Dalle, 'L'arbitrage, une justice alternative pour une nouvelle offre de justice' (2020) 7-8 *La Semaine Juridique*, 12.

grounds of either 'legal impediment or privilege (…) legal or ethical rules' or 'special political or institutional sensitivity'. There is alas no space here to look further at this very interesting question.

In any case, the worker arbitrators in their arbitral hives are not only receivers of the data forming the subject matter of the arbitration, they also are the processors of this data: like the worker bees processing the pollen stored in the hive to make the honey.

II. Privacy in the Arbitrator's Data Processing Activity

What does "Privacy" mean? Privacy is the fair and authorised processing of personally identifiable information. Personal information is any information that can be used to identify or contact an individual or can be reasonably linked to a specific individual, device, or computer. Processing is any action that can be performed in relation to that data: so, processing personal information includes collection, storage, use, sharing, organization, display recording, collation, copying, consultation, erasure, destruction and alteration. Whilst confidential information is an label imposed to signify control of access, personal Information is an organic label: it speaks to the substance of the information. In other words, while confidentiality will apply to data, privacy will apply to persons.

The personal data protection imperative has been taken up by the European Union. The European Parliament has adopted EU Regulation 2016/679 on the Protection of Natural Persons with regard to the Processing of Personnel Data and on the Free Movement of Such Data, named "GDPR" (General Data Protection Regulation). In France, a law was adopted in 2018 to adapt domestic legislation to the European Regulation.

The question arises as to whether online arbitration, and arbitrators in particular, are GDPR-proof. The answer is no, as I will now explain. On this subject I refer readers to the *Club des Juristes*' Working Group Report published in 2019 on Online Arbitration (pages 89-103).

A brief reminder of the provisions of the GDPR may be useful.

As stated in the Report, the GDPR requires any entity having to process the personal data of a natural person to obtain his or her prior consent and to ensure compliance with the protection provided to natural persons by the GDPR.

The right of natural persons includes the right to transparency, the right to access their data, to rectify and erasure them, the right to restrict processing, the right to data portability, the right to object and the right not to be subject to an automated individual decision.

As noted in the report of the Club des Juristes, 'such protection can be difficult to reconcile with the reality of arbitration, notably in view of the confidentiality principle that dominates arbitral procedures, and the need for a court to be able to reach a decision without essential data being withdrawn from it' (p. 89 of the Report)[12]

Furthermore, the GDPR applies:

- To the processing of personal data in the context of activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not,
- To the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: (i) the offering of goods or services, irrespective of whether ta payment of the data subject is required, to such data subjects in the Union, or (ii) the monitoring of their behaviour as far as their behaviour takes place within the Union.

Accordingly, any arbitrator, if established within the European Union, is in principle subject to the GDPR to the extent to which they process personal data during the arbitral procedure.

Examples of personal data listed by the European Commission include: a name and surname, a home address, an email address, an identity card number, location data etc.

Accordingly, any information, even professional, exchanged as part of an arbitration procedure and containing information capable of identifying an individual is considered to be personal data for the purposes of the GDPR: that concerns the documents exchanged by the parties containing such information, and also briefs, witness statements, expert reports and the award itself.

All such documents, if capable of identifying individuals can therefore be subject to the provisions of the GDPR [13].

Processing means any operation performed on personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use disclosure by transmission etc. (Article 4-2 of the GDPR).

---

12 See also, Paisley, 'It's All About the Data: The Impact of the EU General Data Protection Regulation on International Arbitration' (2018) 41 *Fordham Int'l L.J.*, 841 (856); Paisley, 'Managing Arbitration Data under the GDPR' (2018) *Global Arbitration Review*.

13 Le Club des Juristes, Working Group Report, *Online Arbitration*, 2019, 90.

Therefore, during the arbitral procedure, the collection and examination of documents, transfer of documents to an attorney or expert, exchange of documents between the parties or the disclosure of evidence ordered by the Tribunal are all likely to be considered as "processing activities" within the meaning of the GDPR[14].

A controller of data processing under the GDPR is defined as 'the natural or legal person, public authority, agency or another body which, alone or jointly with others, determines the purposes and means of the processing of personal data' (Article 4-7 of the GDPR).

The task of the controller is to ensure that the personal data is 'processed lawfully, fairly and in transparent manner', 'collected for specified, explicit and legitimate purposes, and not further processed in a manner that is incompatible with these purposes', 'adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed', 'accurate and necessary, kept up to date', 'processed in a manner that ensures appropriate security of the personal data' and retained for a limited duration (Art. 5 GDPR)[15].

As stated in the ICC Note to the Parties and Arbitral Tribunals (2021 version)[16], in performing their duties under the ICC Arbitration Rules, arbitral tribunals have to collect and process such personal data. For this purpose, personal data of this kind may be transferred by or to the various offices of the Secretariat in and out of the European Union.

Accordingly, because of the very nature of their functions, arbitrators are the actors in the arbitral procedure likely to be considered as controllers under the GDPR.

In their capacity as controllers under the GDPR, the arbitrators are subject to the following main obligations:

- To set up a cybersecurity system (Article 32): controllers are required to implement appropriate technical and organisational measures in order to guarantee a security level in keeping with the risk, including anonymisation and encryption of the personal data or measures intended to restore the availability of personal data. We will come back to this matter in the final part of this article.
- Data minimisation (Article 5): this is the principle whereby 'personal data may only be processed if, and insofar as, the processing purposes

14 *Ibid*, 91.
15 Ibid.
16 ICC, *Note to the Parties and the Arbitral Tribunals on the Conduct of the Arbitration under the ICC Rules of Arbitration*, 1 January 2021.

cannot be attained by the processing of information that does not contain personal data'[17]. Controllers must therefore ensure that the collected data is necessary for the processing, while reducing the categories as well as the volume of data processed to a minimum.

- Right to transparency (Articles 13 and 14): every controller must provide the data subject with specific information. This includes: the contact details of the controller and processor, the purposes of the processing and the respective basis, the legitimate interests pursued by the controller, where applicable, any intention of transferring personal data to a third country, the period for which the personal data will be stored and/or the criteria used to determine that period, the existence of the right to request from the controller access to and rectification and erasure of personal data, or restriction of processing concerning the data subject, or to object to processing as well as the right to data portability, the existence of the right to withdraw consent at any time, and the right to lodge a complaint with a supervisory authority[18].
- Right to rectification and to erasure (Articles 16 and 17): the data subject has the right to obtain from the controller the rectification of personal data concerning him or her. Such right cannot be exercised when the data processing is necessary for the establishment, exercise, or defence of legal claims. Accordingly, an arbitral procedure will be exempted from this obligation if the data is considered necessary for the exercise and defence of the rights of the parties, and that its erasure could undermine this.

The GDPR mentions six specific cases in which the processing of data is lawful (Art. 6):

- The data subject has given consent to the processing of the personal data for one of more specific purposes,
- Processing is necessary for the performance of a contract,
- Processing is necessary for compliance with a legal obligation to which the controller is subject,
- Processing is necessary to protect the vital interests of the data subject or of another natural person,

17 Conseil National des Barreaux, Guide Pratique – Les Avocats et le Règlement Générale sur la Protection de Données (RGPD), March 2018.

18 Le Club des Juristes, Working Group Report, *Online Arbitration*, 2019, 93.

- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller,
- Processing is necessary for the purposes of the legitimate interests pursued by the controller of by a third party.

According to the Report of the Club des Juristes' Working Group on Online Arbitration: 'Data processing in connection with an arbitral procedure must be considered "lawful" since it is necessary for the fulfilment of a contract, to meet a legal obligation, or for the purposes of the legitimate interest pursued by the controller'[19]. I share this opinion.

Article 23 authorises Member States to provide for exceptions allowing data processing in contexts other than those indicated in the Regulation. Ireland adopted an exception to allow a limitation of the rights of data subjects in connection with judicial or arbitral proceedings. For the sake of arbitrators' peace of mind, the other European countries should do the same.

Finally, the GDPR only authorises the transfer of personal data to a country other than a Member State when the European Commission considers that the protection level provided by the third country is adequate, the controller or processor has provided appropriate safeguards for the data transfer, a court orders the data transfer in compliance with the treaty, or one of the exemptions under Article 49 applies, authorising data transfer to a third country when 'the transfer is necessary for the establishment, exercise or defence of legal claims'. This last exemption will enable data to be transferred to a third country in connection with arbitration.

In consideration of all these GDPR rules applicable to the arbitrators in their capacity as controllers in the processing of personal data in arbitration proceedings, the ICC added a section in its Note to the Parties and the Arbitral Tribunals on the Conduct of Arbitral Procedures addressing the subject of protection of personal data. In this Note, the ICC deals with the necessary consent to be obtained from the personal data subjects as well as with the ways the arbitrators must comply with their obligations under the GDPR.

In the first place, therefore, the ICC envisages that all the actors in arbitration procedures, and the arbitrators in particular, should agree on the fact that personal data needs to be collected, transferred and stored for the purposes of the arbitration proceedings and that this data may be

19 *Ibid*, 95.

published in the event of publication of an award, procedural order and dissenting and/or concurring opinion.

The ICC Note goes on to invite arbitrators, and in their capacity as controllers, to:

- remind the parties, representatives, witnesses, experts and any other individuals appearing before it that the GDPR or other data protection laws and regulations apply to the arbitration, that their personal data may be collected, transferred, published and archived pursuant to the arbitration agreement or the legitimate interests in resolving the dispute and that arbitration proceedings operate fairly and efficiently,
- draw up a data protection protocol to that effect,
- ensure that only personal data that is necessary and accurate for the purposes of the arbitration proceedings is processed and that any individual whose data is collected and processed in the context of an arbitration shall be able at any time to apply to the appropriate data controller to exercise his right of access and that inaccurate data be corrected or suppressed, in accordance with the applicable data protection laws and regulations,
- ensure that all those acting on their behalf put in place appropriate technical and organisational measures to ensure a reasonable level of security for the arbitration, taking into account the scope and risk of processing, the state of the art, the impact on data subjects, the capabilities and regulatory requirements of all those involved in the arbitration, the costs of implementation, and the nature of the information being processed or transferred, including whether it includes personal data or sensitive business, proprietary or confidential information.

Lastly, the Note provides that once the arbitration procedures are completed, the arbitrators may retain the personal data processed during the proceedings for as long as they keep the case file in their archives pursuant to applicable laws, such duration having to be communicated to the parties and the ICC.

According to the ICC Note, the arbitrators are therefore invited to address the question of the processing of personal data with the parties and counsel at the beginning of the arbitral procedure. As far as I am concerned, as a President of arbitral tribunals, I now include in the Terms of Reference an article on protection of personal data, whereby the arbitrators are authorized to collect, process, transfer, store and archive this data if included in the awards, procedural orders and emails likely to be archived after the end of the procedure.

In addition to a provision in the Terms of Reference on personal data protection, and to better protect this data, the use of an arbitration platform can reduce the risks of data breaches.

Indeed, as suggested in the above-mentioned Protocol for Online Case Management in International Arbitration, published by arbitration practitioners in July 2020, the use of a Platform in arbitration proceedings can enable personal data exchanged in the proceedings to be:

- processed only in those ways that have been agreed by the parties or directed by the arbitrators,
- processed only for the legitimate purposes for which they were expressly collected (i.e. the proceedings),
- shared only with those parties that need to process it (if a challenge is raised as to which party received the data, the Platform will help establish the trail of the data flow),
- kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed,
- effectively destroyed once the proceedings have ended.

Because of the obligations of privacy, arbitrators are no longer only responsible, but they also are accountable. Responsibility will be enforced through damages granted to victims. Accountability will be enforced through administrative fines. An arbitrator who fails to comply with his or her obligations under the applicable data protection regulations will be liable to the data subject concerned (Article 82 of the GDPR). Moreover, if his fault had consequences on the arbitration proceedings, he could also be liable to the parties to the proceedings, unless he benefits from an exclusive liability clause (which can be set aside in case of gross negligence and inexcusability). The arbitrator may also be exposed to administrative fines (Article 83 of the GDPR).

In their arbitral hives, we noted that worker arbitrators are both storing and processing arbitral data. But arbitrators are not only workers in their hives. Once the data (just like pollen) is brought into the arbitral hives, the data needs to be protected from external predators. In the same way that soldier bees protect the hives from external attacks, arbitrators will assume the role of soldiers in the fight against cyber-attacks, and therefore contribute to the security of the arbitral process.

B. The Contribution of the Soldier Arbitrators to the Security of the Arbitral Hives

What does "Security" mean? Security means all measures likely to be implemented to avoid:

- security incidents, i.e. any event that may compromise the confidentiality, integrity, or availability of data, and
- security breaches, i.e. any security incident that results in unauthorized access to data and requires that notice be given to persons whose data has been compromised.

Accordingly, cybersecurity is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks.

If digital data is the pollen that feeds the labours of the worker arbitrators in the digital arbitral hives, it becomes the nectar that feeds the appetite of predators outside the hive. As I observed in my introduction, these predators do exist. Many arbitrators do not seem to realize that the material they deal with, the data they receive and exchange in arbitration proceedings, constitutes a real asset, which malicious persons may want to appropriate for their own purposes or to retail on the Dark Web through mafia networks.

Indeed, international arbitrations involve parties which are multi-national groups or governments or state entities and which as such hold valuable, highly commercial and sensitive information[20]. This information will all be shared within a space and during a limited period of time (the arbitral procedure) and this may facilitate the work of hackers who thereby gain access to valuable economic digital data. What is more, the variety of information technology used in arbitrations, including emails, cloud storage, hearing room technologies and software for interpreting,

20 de Westgaver, 'Cybersecurity in International Arbitration – A Necessity and An Opportunity For Arbitral Institutions' (2017) *Kluwer Arbitration* Blog, available at http://arbitrationblog.kluwerarbitration.com/2017/10/06/cyber-security/; Rahman, 'The Role of Arbitral Institution in Cybersecurity and Data Protection in International Arbitration' (2020) *Kluwer Arbitration Blog,* available at http://arbitrationblog.kluwerarbitration.com/2020/11/24/the-role-of-arbitral-institutions-in-cybersecurity-and-data-protection-in-international-arbitration/.

translating, document presentation, etc., provides a wide landscape for cyber-security threats[21].

The consequences of these cyber-attacks may be very serious for the parties involved in the arbitrations and lead to loss of personal/commercial data, money, intellectual property and reputation; their market value may fall and regulatory actions ensue. What is more, as the literature has rightly noted, after a cyber-security incident, the participants may find it difficult to trust the arbitration process (and the arbitrators) and may also question any data that is presented for its authenticity[22]. Similarly, the ICCA-NYC Bar-CPR Protocol on Cybersecurity in International Arbitration (2020) identifies several consequences that may result from inadequate attention to information security:

- Economic loss to individuals whose commercial information or personal data is compromised,
- Loss of integrity of data, or questions about the reliability and accuracy of data,
- Unavailability of data, networks, platforms, or websites due to disruption caused by a security incident,
- Potential liability under applicable law and other regulatory frameworks,
- Reputational damage to parties, arbitrators, arbitral institutions, and third parties, as well as to the system of arbitration in general[23].

Arbitration procedures cannot ignore these cyber-threats. This applies especially to arbitrators who, even though a significant proportion of their number are reluctant to actively engage in assessing cybersecurity risks and designing appropriate measures (relying on the parties)[24], will have to accept their role as soldier arbitrators against Cybercrime in their arbitral duties. In this respect, some practitioners tend to consider that the preservation and protection of the legitimacy and integrity of the arbitration

21 Mirani, 'Tackling Cyber Security Threats in Arbitration – Have We Done enough?' (2020) ICAR, available at https://investmentandcommercialarbitrationreview.com/2020/09/tackling-cyber-security-threats-in-arbitration-have-we-done-enough/.

22 *Ibid*.

23 ICCA, *ICCA-NYC Bar-CPR Protocol on Cybersecurity in International Arbitration*, 2020, 8-9.

24 de Westgaver, 'Cybersecurity in International Arbitration: Don't be The Weakest Link' (2019) *Kluwer Arbitration Blog,* available at http://arbitrationblog.kluwerarbitration.com/2019/02/15/cybersecurity-in-international-arbitration-dont-be-the-weakest-link/.

process may constitute an ethical obligation on the part of arbitrators (*ICCA-NYC Bar-CPR Protocol on Cybersecurity in International Arbitration* (2020) (p. 16)).

Arbitrators must therefore take into consideration the general IT environment of an arbitral procedure, in order to assess whether, in the light of the specific feature of a given dispute, special consideration should be paid to Information Security Measures (known as ISM). For instance, under the new LCIA Arbitration Rules (Article 30 A), arbitrators are required to consider whether it is appropriate to adopt not only means to address the processing of personal data produced or exchanged in the arbitration in light of applicable data protection or equivalent legislation, but also specific information security measures to protect the physical and electronic information shared in the arbitration.

When should these ISM issues be addressed by the arbitrators with the parties, if they are needed? The best time would be at the case management conference, at the beginning of the arbitral procedure. This is what the ICC suggests in its ICC Commission report on Information Technology in International Arbitration, published in 2017 (page 20), as well as what the ICCA-NYC Bar-CPR Protocol on Cybersecurity in International Arbitration (2020) suggests (Schedule D). According to the ICCA Protocol, at the CMC the arbitrators should be prepared to:

– Engage the legal representatives in a discussion about reasonable information security measures,

– Discuss the ability and willingness of the members to adopt specific security measures,

– Address any disputes about reasonable ISM, express their own interest in preserving the legitimacy and integrity of the arbitration process, considering the parties' concerns and preferences, the capabilities of any administering institution (pp. 26-27 of the Protocol).

After the CMC, if the hearing is to be held online, a Protocol on the necessary arrangements may include provisions on security.

In their assessment of the needs for specific ISM in an arbitration, all arbitrators should bear in mind that the ISM must be designed to protect what is called the CIA-Triad, i.e. Confidentiality, Integrity and Availability, where:

– as already mentioned, Confidentiality means protecting information from unauthorised access,
– Integrity means ensuring that the information is accurate and that systems function as intended,

– Availability means guaranteeing uninterrupted access to information and systems.

Arbitrators should be considered as having the authority to determine the ISMs applicable to arbitrations. With a view to this, they should respect any engagement by the parties on the ISM to be employed, subject to overriding legal obligations or any significant countervailing considerations. Conversely, the parties must not be authorised to bind unilaterally the arbitrators. One reason for the arbitrators not to accept the ISM proposed would be the need to ensure proportionality. The measures should be proportionate to the arbitration and the IT resources that both parties can afford[25].

What are the means available for arbitrators to address security concerns?

The best way will be for the arbitrators to propose that the parties agree on an ISM Protocol. The purpose of this Protocol will be to provide a framework for incorporating and implementing reasonable ISM, i.e. both technical and organizational measures to secure against cyber security threats[26]. The ISM must be tailored to the risks present in the arbitration[27] and to the size of the entities involved in the arbitration. An author[28] has summarized the main features of the protocol proposed by the ICC to which the actors of an arbitration may refer in order to address their security concerns:

– The ICCA protocol prescribes that parties must exercise their autonomy to agree upon reasonable ISM. Thereafter, the arbitrators have final authority to determine the ISM applicable to arbitration,
– The arbitrators may depart from parties' agreement, to raise or lower the standards of ISM, based on capabilities of arbitrators and institutions, interest of third parties, such as witnesses, etc. and of legitimacy/integrity of arbitral Process: that leads to two observations:

25 ICC, *ICC Commission Report: Information Technology in International Arbitration*, 2017, 5.

26 Mirani, 'Tackling Cyber Security Threats in Arbitration – Have We Done enough?' (2020) ICAR, available at https://investmentandcommercialarbitrationreview.com/2020/09/tackling-cyber-security-threats-in-arbitration-have-we-done-enough/.

27 ICCA, *ICCA-NYC Bar-CPR Protocol on Cybersecurity in International Arbitration*, 2020, 22-24

28 Ibid.

  - first, arbitrators shall be selected in consideration of their capability to meet security standards. Indeed, arbitrators practising as single practitioners may not have access to sufficient IT services[29].
  - encryption of emails, share-file services, or use of USB keys to store and exchange data may be minimum ISM on which parties and the arbitrators may agree, if need be.
- Once the ISM are agreed upon, it is the duty of all the persons involved in the arbitration having access to any arbitration-related information, to implement them.
- Arbitrators shall ensure that any person involved in the arbitration is aware and is following the duly agreed ISM.

The last point is essential in the mission of our soldier arbitrator. Indeed, security in arbitral proceedings ultimately depends on the decisions and actions of all involved. Actions by any individual can be the cause of an information security incident, no matter the setting in which they take place or the infrastructure available to them. Indeed, as observed in the ICCA Protocol, many security incidents result from individual conduct rather than a breach of systems or infrastructure[30]. In other words, cybersecurity is only as robust as the 'weakest link' in the chain[31]. And to use again an insect metaphor, a good way to understand the risk run because of the weakest link is to observe how cockroaches use the lack of coordination between inhabitants of a building to survive, by taking refuge in the non-disinfected space of a building, due to the refusal of one inhabitant to mobilize in the fight against the invader. To fight an invasion of cockroaches, all the occupants of a building have to be mobilised. Transposed to cyberworms and other cyberviruses, this means that the inadequate security arrangements of one of the participants in an arbitration procedure can undermine the entire process.

One way to protect the arbitration process against security incidents and breaches may again be the use of Platforms. Arbitrators may propose such a tool at the CMC. A Platform may help level up the overall security of the custody chain as long as the relevant functions are enabled and used. Such

29 On the selection of arbitrators: ICC, *ICC Commission Report on Information Technology in International Arbitration*, 2017, 6-7.

30 ICCA, *ICCA-NYC Bar-CPR Protocol on Cybersecurity in International Arbitration*, 2020, 10.

31 Working Group on LegalTech Adoption in International Arbitration, *Protocol for Online Case Management in International Arbitration,* July 2020, para. 24.

a Platform may also reduce security and privacy risks when users transfer data through the Platform rather than by email.

Finally, as soldiers, the arbitrators in online arbitrations may not only combat the risks of cybersecurity incidents but may also penalise a participant for having violated the security measures. The ICCA Protocol recognises the power to arbitrators to allocate the additional costs arising from the security incident among the parties at their discretion and to impose penalties on the parties. More generally, a participant who has violated the ISM may incur liability to the other participants if they suffered damages as a result of the violation.

In conclusion, arbitrators undoubtedly do face new challenges in cyberspace. But these challenges are not at all insurmountable. And if arbitrators feel uneasy, they can fly, like a bee, to Lisbon, and de-stress by enjoying what Pessoa described as … the city's spray of colours under the sun!

Bibliography

Roger Alford, 'The Virtual World and the Arbitration World' (2001) 18 *Journal of International Arbitration*, 449.

Marie-Charlotte Dalle, 'L'arbitrage, une justice alternative pour une nouvelle offre de justice' (2020) 7-8 *La Semaine Juridique*, 12.

Allison Goh, 'Digital Readiness Index for Arbitration Institutions: Challenges and Implications for Dispute Resolution under the Belt and Road Initiative' (2021) 38-2 *Journal of International Arbitration*, 253.

Marc Henry, 'Infraction pénale et confidentialité de l'arbitrage : devoirs et obligations des arbitres et des conseils' (2019) 2019-1 *Revue de l'Arbitrage*, 65.

Saniya Mirani, 'Tackling Cyber Security Threats in Arbitration – Have We Done enough?' (2020) ICAR, available at https://investmentandcommercialarbitrationreview.com/2020/09/tackling-cyber-security-threats-in-arbitration-have-we-done-enough/.

Kathleen Paisley, 'It's All About the Data: The Impact of the EU General Data Protection Regulation on International Arbitration' (2018) 41 Fordham Int'l L.J., 841 (856).

Kathleen Paisley, 'Managing Arbitration Data under the GDPR' (2018) *Global Arbitration Review*.

Diana Rahman, 'The Role of Arbitral Institution in Cybersecurity and Data Protection in International Arbitration' (2020) *Kluwer Arbitration Blog,* available at http://arbitrationblog.kluwerarbitration.com/2020/11/24/the-role-of-arbitral-institutions-in-cybersecurity-and-data-protection-in-international-arbitration/.

Claire de Westgaver, 'Cybersecurity in International Arbitration – A Necessity and An Opportunity For Arbitral Institutions' (2017) *Kluwer Arbitration Blog*, available at http://arbitrationblog.kluwerarbitration.com/2017/10/06/cyber-security/

Claire de Westgaver, 'Cybersecurity in International Arbitration: Don't be The Weakest Link' (2019) *Kluwer Arbitration Blog,* available at http://arbitrationblog.kluwerarbitration.com/2019/02/15/cybersecurity-in-international-arbitration-dont-be-the-weakest-link/.