

## Smart Arbitration in the Service of Cybersecurity

**Kenza BOUMALA \***

Institution Law Laboratory  
Djilali LIABES University - Sidi Bel Abbas,  
Algeria

[Boumalakenza@gmail.com](mailto:Boumalakenza@gmail.com)

**Adiba Linda BENTURQUIA**

Institution Law Laboratory  
Djilali LIABES University - Sidi Bel Abbas,  
Algeria

[linda-allal-benturquia@hotmail.fr](mailto:linda-allal-benturquia@hotmail.fr)

Date of submission: 12/11/2024 - Date of acceptance: 06/12/2024 - Date of publication: 28/12/2024

**Abstract:** Artificial intelligence (AI) is considered one of the most significant achievements of the Fourth Industrial Revolution due to its extensive applications across various sectors. With the rapid advancement of technology, electronic contracts-especially commercial ones.

This requirement has spurred the codification of a legal scheme distinct to these digital contracts. Digital arbitration centers, which decide disputes between the contracting parties using AI technology, that is 'smart arbitration'.

Nevertheless, a digital environment is also susceptible to cyberattacks. Several technical solutions have been developed to prevent such instances of insecurity and provide for the data privacy and the security of smart arbitration processes.

**Keywords:** Artificial intelligence, smart arbitration, cybersecurity, cyberattacks, data privacy.

\*Corresponding author: Kenza BOUMALA.

## **Introduction:**

As our cursory assessment of legal affairs exposed, the rise of smart arbitration – the idea of using artificial intelligence (AI) and blockchain technologies within the realm of dispute resolution to solve disputes outside the traditional judiciary – should be seen as an extension of a wider phenomenon: the increasing use of digital systems, and their unquestioned acceptance by all involved. It is quicker, more transparent, and cheaper than conventional dispute-resolution systems. However, an array of legal and ethical issues arise with these new technologies: not only will there be a need to ascertain the propriety of decisions being made by intelligent systems, to protect confidential personal information from breaches of data security, or to avoid potential algorithmic prejudices that might ultimately undermine the quality of justice.

This study aims to analyze the concept of smart arbitration and differentiate it from traditional electronic arbitration, with a particular focus on its applications within cybersecurity. Additionally, the research seeks to provide a comprehensive framework to address the challenges posed by this advanced arbitration model at both technical and legal levels. It explores ways to enhance intelligent systems to promote justice and ensure the protection of individuals' rights amidst continuous technological development, especially with the growing use of AI. The core of the issue raised by this study is therefore how to make smart arbitration systems compliant with current legal and ethical standards without sacrificing the effectiveness and efficiency that technology of the smart era offers. In short: can smart arbitration assure cybersecurity?

## **Objectives of the Study**

1. Developing a concept of smart arbitration, clarifying the difference between smart arbitration, electronic arbitration, and traditional arbitration.
2. Examining the legal and technical obstacles that smart arbitration would face, especially when it comes to trust in decision taking by intelligent systems.
3. How AI and smart arbitration could assist with arbitration procedures, and enhance efficiency.
4. Exploring ethical challenges, such as algorithmic bias, and its implications for justice.
5. Making suggestions to improve smart arbitration by proposing new legislation and legal principles that would promote the implementation of AI in the process of resolving conflicts.
6. Look at how smart arbitration may be used in the context of cybersecurity as a way of improving both security and forensic threat prediction.

## **Study Methodology:**

In order to analyze and explain the concept of smart arbitration, its applications in the field of cybersecurity, and the technical and legal challenges it presents, the study used two main methodologies: the descriptive method and the inductive method. The inductive method was used to review existing models of smart arbitration systems and the strategies implemented to address cybersecurity challenges related to data security and emerging threats in recent years.

As a result, this study is divided into two sections: the first section discusses the concept of smart arbitration, and the second section examines its functions within cybersecurity and the challenges posed by them.

### **I.THE CONCEPT OF SMART ARBITRATION AND ITS APPLICATIONS**

With advancing technological development, and the emergence of and its realization of new ideas in the field of arbitration as well in all financial fields, at the hands of major tech giants such as Google Technology, Microsoft, and on our mobile devices, the development of information and communication technology in the future cannot be predicted. In this context, the design and development of third smart arbitration continues to represent a remarkable revolution, and a promising branch in history of arbitrations and dispute resolutions as a whole, which is an important innovative idea that represents a huge global opportunity for opening new international doors for the ability of providing more effective ways to handle the conflicts and disputes, to reach a commitment to settle the conflict, which cannot be, and will never be achieved by state courts that intervene excessively. Wise arbitration is the last phase in the process of electronic arbitration that followed electronic commerce. Wise arbitration refers to the sophisticated, and latest form of electronic arbitration, which involves all legal or administrative procedures are conducted through a program that is coded and run completely by computers. The program will mandate the production of legal statements once all disputes points inserted under rules of electronic arbitration rules. It means that we are talking about the phase of arbitration performance automatically by computer, and its achievement without any intervention at all from any human minds, which will reduce the duration of time of bureaucratic intervention, and will always contribute to more saving of funds. In this context, the aims of this article is about presenting a comprehensive overview of the emergence of smart arbitration and its differences from the electronic arbitration, presentation of explanation for the mechanisms and stages of the third smart arbitration, and explanation of the benefits of such legal form, such as efficiency and its technical security, in addition to its easiness and access to all documents and records included in every arbitration number. Such topics will be divided into 2 parts; the first part will deal with the electronic arbitration, while the second part will deal with the cybersecurity. The details are as follows:

#### **I. 1- The Concept of Smart Arbitration**

Given the accelerating pace of technological change, the availability and potential impact of new directions in arbitration – such as ‘smart arbitration’ by artificial intelligence – are an important next step in the story of the human struggle to resolve our differences. This new arbitration has opened vast new frontiers globally and provides means to resolve disputes in far more efficient ways that courts or other enforcement bodies cannot.

Smart arbitration is regarded as the last development in electronic arbitration, whereby arbitral proceedings are conducted entirely by means of the software programs generating legal decisions when all the contested points are keyed-in according to rules of electronic arbitration. The last phase means that arbitration is processed automatically without human beings and bypasses a lot of bureaucratic procedures which require long months, even years, compared with considerable sums of money of real arbitration.

In this article, I am going to provide an overview of the smart arbitration, highlighting its difference from other types of electronic arbitration, as well as explaining the mechanisms and stages of smart arbitration in addition to its advantages such as improving its efficiency, enhancing the technical security of the arbitration and making all its documents and records very much accessible.

The main idea will consider the differences between electronic arbitration and cybersecurity. Firstly, I think that the two arguments are opposites. Electronic arbitration deals with the buying and selling of arbitration services, while cybersecurity focuses on protecting data and other computer functions from unauthorized access. Secondly, I disagree that the two arguments create an 'either/or' argument. Therefore, I think that electronic arbitration aims to reduce remedies for commercial disputes by using arbitration agreements. On the other hand, cybersecurity work deals with protecting important data and computer functions from unauthorized access. These two are the opposite of each other. For example, when the government wants to stop news evasion, they use electronic technology. This is because newspapers do not have their own information or messages; they use electronic devices to send messages.

### **I. 1.1- Definition of Smart Arbitration**

Arbitration is defined as "a legal system by which a binding decision is made in a legal dispute between two or more parties by an individual or individuals who derive their authority from the agreement of the disputing parties"<sup>1</sup>. Arbitration is 'a system for the resolution of disputes between two or more parties that is based on the agreement of the parties to be bound by the decision of a third party or parties'. The arbitrators are either directly selected by the parties (free arbitration) or appointed by a third party, with the arbitration period determined by the agreement of the parties or by law. Arbitrators issue a binding decision without resorting to the formal judiciary, which contributes to the continuity of economic and social relations between the parties.<sup>2</sup>

According to the Egyptian Court of Cassation, arbitration is: [a] legal contractual system independent of the state courts where the parties may designate the arbitrators to settle their dispute concerning their contractual or non-contractual disputes according to law or principles of justice.<sup>3</sup>

The Egyptian Arbitration Law of 1994 states that an arbitration is 'conducted by the free will of the parties' either the body itself is an organization, a permanent centre or otherwise.

Whether arbitration is conducted through traditional procedures (face-to-face), electronic procedures (email, for example) or with the help of smart arbitration technology, which facilitates the automation of arbitration proceedings and agreements, parties put their complete trust in the goodwill and impartiality of the arbitrator.

---

<sup>1</sup> Fathi Wali, The Law of Arbitration in Theory and Practice, First Edition, Al Maaref Establishment, Alexandria, 2007, p. 13.

<sup>2</sup> Sayed Ahmed Mahmoud, Electronic Arbitration in the New Emirati Law No. 6 of 2018, Journal of Legal Sciences, Sharjah University, Vol. 19, Issue.

<sup>3</sup>[[https://wwwcc.gov.eg/judgment\\_single?id=111742837&&ja=300721](https://wwwcc.gov.eg/judgment_single?id=111742837&&ja=300721)]([https://wwwcc.gov.eg/judgment\\_single?id=111742837&&ja=300721](https://wwwcc.gov.eg/judgment_single?id=111742837&&ja=300721))

### I. 1.2- The Difference Between Electronic Arbitration and Smart Arbitration

Although electronic arbitration and smart arbitration both utilize electronic means<sup>4</sup>, they differ significantly. Electronic arbitration relies on digital tools to conduct arbitration but still depends on human arbitrators known to the parties. In contrast, smart arbitration uses computer programs based on artificial intelligence, which reduces the role of human arbitrators in the arbitration process.

Smart arbitration refers to arbitrations that are conducted begins to end on smart arbitration platforms, such as on Ethereum-based platforms. Smart arbitration relies on full or partial digitalization of arbitration processes including the election of arbitrators, admission of evidence, and the rendering of decisions. In this respect, it is distinct from e-arbitration that comprises a mix of human and digital technologies.

The arbitrators of the arbitration committee in smart arbitration are randomly selected from the arbitration committee members according to the encrypted token, and the decision is made through voting by the majority of the arbitrators of the arbitration committee. Different from electronic arbitration, the voting of arbitrators in smart arbitration does not mention the quorum. In addition to the online arbitration modes in the development of electronic arbitration and smart arbitration, there is an offline arbitration mode, secret arbitration.

In short, most of what we refer to as smart arbitration relies on encryption and full automatisisation, the main distinguishing features that make it considerably different from mere electronic arbitration compared with essentially paper-based traditional arbitration that happens to rely on electronic tools.<sup>5</sup>

### I. 1.3- Advantages of Smart Arbitration

#### – Low Cost:

Smart arbitration is less costly than traditional arbitration and ordinary courts, as everything is done digitally, eliminating the need for travel or securing venues for arbitration sessions.<sup>6</sup>

---

<sup>4</sup> Although current decisions in smart arbitration still involve a human element, due to the lack of fully verified and legally assessed digital arbitration bodies so far, the anticipated future suggests the possibility of completely eliminating human involvement in smart arbitration. This can be achieved by relying on computer software using pre-programmed algorithms to deliver appropriate rulings for each anticipated case. In this way, the smart arbitration process becomes fully automated without human intervention, including the selection of specialized arbitration platforms, the presentation of evidence, the submission of defenses, and even the issuance of judgments. This futuristic concept is what this study aims to explore and is what distinguishes smart arbitration from traditional electronic or human arbitration.

<sup>5</sup> Mohamed Rabie Fath El Bab, *Artificial Intelligence Contracts: Their Origin, Concept, Characteristics, and Dispute Resolution through Blockchain Arbitration*, p. 240.

<sup>6</sup> Pachahara (S.) and Maheshwari (C.), *Dispute Resolution on Blockchain: An Opportunity to Increase Efficiency of Business Dispute Resolution*, Conflict Studies Quarterly, Babeş-Bolyai University, Romania, Issue 39, April 2022, p. 75. Available at: [\[http://www.csq.ro/wp-content/uploads/CSQ-39.pdf\]](http://www.csq.ro/wp-content/uploads/CSQ-39.pdf)(<http://www.csq.ro/wp-content/uploads/CSQ-39.pdf>).

– **Short Timeframe:**

Smart arbitration platforms save time thanks to fast digital procedures compared to traditional arbitration or courts.<sup>7</sup>

– **Technical Security:**

Distributed ledger technology and the full encryption of data by smart arbitration ensures high security. This technology of intelligence also makes the breach much harder, because shared distributed ledgers store data across the network, and encryption is cross-checked.

– **Ease of Access to Information:**

Smart arbitration provides easy access to all information and documents related to self-executing contracts, ensuring data accuracy through encrypted verification.<sup>8</sup>

– **Error Reduction:**

Smart arbitration relies on a decentralized system that minimizes human intervention<sup>9</sup>, increasing transparency and fairness in decisions, especially in disputes related to supply chains and logistics services.<sup>10</sup>

– **Fairness:**

Smart arbitration ensures fairness in dispute resolution through fully encrypted procedures, while guaranteeing the anonymity of arbitrators and disputing parties.

#### **I. 1.4- Smart Arbitration Procedures**

Smart arbitrations are run entirely online (and encrypted). When a party or parties to an agreement have a dispute, they send a request to the smart arbitration dispute-resolution service they agreed to use in the first place (eg, Kleros). One smart option, proposed by Kleros' current platform, is that the initiating party is given an opportunity to propose a compromise to the conflict; the other party has 24 hours to respond with a compromise of their own, or otherwise commit to the dispute-resolution process. This ensures that the 'good faith' premise of an agreed contract remains intact.<sup>11</sup>

This indirectly reinforces the concept of the principle of good faith in contract performance, a principle acknowledged by the Algerian Civil Code under Article (107),

---

<sup>7</sup> Chevalier (M.), From Smart Contract Litigation to Blockchain Arbitration: A New Decentralized Approach Leading Towards the Blockchain Arbitral Order, *Journal of International Dispute Settlement*, Vol. 12, Issue 4, December 2021, p. 567. Available at: <https://academic.oup.com/jids/articleabstract/12/4/558/6414874?redirectedFrom=fulltext>](<https://academic.oup.com/jids/articleabstract/12/4/558/6414874?redirectedFrom=fulltext>).

<sup>8</sup> Pachahara and Maheshwari, op. cit., p. 73, p. 76.

<sup>9</sup> In the same sense, see: Pachahara and Maheshwari, op. cit., p. 75.

<sup>10</sup> Pachahara and Maheshwari, op. cit., p. 77.

<sup>11</sup> Buchwald (M.), Smart Contract Dispute Resolution: The Inescapable Flaws of Blockchain-Based Arbitration, *University of Pennsylvania Law Review*, Vol. 168, 2020, J.D., University of Pennsylvania Law School. Available at: [https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=9702&context=penn\\_law\\_review](https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=9702&context=penn_law_review)]([https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=9702&context=penn\\_law\\_review](https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=9702&context=penn_law_review)), p. 1387.

Paragraph 1, which states <sup>12</sup>: "The contract must be executed in accordance with its terms and in a manner consistent with good faith." Similarly, Article (1104) of the French Civil Code<sup>13</sup> states: "Contracts must be negotiated, concluded, and executed in good faith," and this provision is considered part of public policy.

### **I. 2-Cybersecurity Threats**

The arbitration process can only go ahead if the parties do not come to an agreement, at which point the other party is notified of the dispute. The arbitrators are selected at random by the platform, or at the parties' discretion, and all steps are conducted in confidence to preserve the integrity and fairness of the process, as the arbitrators will be unable to know the identities of the parties, and vice versa.

The arbitration rules under its protocol are specific to the regime of the chosen platform, namely the construing law, language and time frame of arbitration, as well as the arbitrators who have to be technical experts in smart arbitration, each possessing the platform's encrypted tokens.

The decisions are determined by a collective vote of the arbitrators, which they are encouraged to cast so as to maximize their chances of getting consensus. The results are explicitly non-binding, which gives the parties the option of appealing, but the fees and nances vary by platform.<sup>14</sup>

#### **I. 2.1-The concept of cybersecurity**

In this section, we will explore the concept of cyberspace and the associated threats. We will begin by defining cyberspace as the domain of digital operations and then address cybersecurity threats in the second section, concluding with a discussion on the various dimensions of cybersecurity.

#### **I. 2.2-Definition of Cybersecurity**

The definition of cybersecurity is 'the process of protecting networks and computer systems from attack, damage or unauthorized access'. It includes the policies and procedures that need to be put in place to prevent or counteract threats such as hacking or a breach of information systems.

Dealing with these threats is known as cybersecurity, defined above by Kemerer Richard A. as 'any measure taken to mitigate the risk of attack or unauthorized access to software, computers, or control systems, including the tools and methods used.

Cybersecurity is the process of protecting human and financial assets that are connected to information and communication technology. The purpose of cybersecurity is to reduce risk,

---

<sup>12</sup> This is reflected in the first paragraph of Article 107 of Law 5-15, dated September 30, 1975, amended and supplemented by Law 07-05, dated May 13, 2007, published in Official Gazette No. 31, dated May 13, 2007, which states: "The contract must be executed in accordance with its terms and in good faith."

<sup>13</sup> Article (1104) of the Civil Code: "Contracts must be negotiated, concluded, and executed in good faith. This provision is part of public policy."

<sup>14</sup> Buchwald, op. cit, pp. 1391-1392.

threats and losses. Cybersecurity also includes safeguarding sensitive information and securing networks, applications and electronic devices from intrusion, alteration and damage.<sup>15</sup>

The word cyber derives from Cyber, meaning ‘relating to computers, information technology and automated control’. Cyberthreats to security are those employing computers to commit sabotage, destroy infrastructure, disrupt defense networks, and penetrate information systems.<sup>16</sup>

Threats in cyberspace cause hazards to social, economic and national security. Not all cyber threats have morality or physical consequences, they might only have social consequences. A cyber threat as per common understanding is can be defined as any malicious activity occurring in the global system of interconnected computer networks that uses internet protocol to communicate. Cyber threats are an increasingly popular way to disrupt peace across the world.<sup>17</sup>

## **II. FUNCTIONS OF SMART ARBITRATION IN CYBERSECURITY AND ITS CHALLENGES**

As the digital age becomes more and more full of threats, smart arbitration can not only expedite the process of cybersecurity but also settle disputes related to cyber issues effectively by integrating artificial intelligence technologies to manage disputes, thereby reducing interventions and increasing transparency during the process. This type of arbitration can be the booming method of managing and settling cyber disputes in the future for merit-based large data processing.

This study addresses the following main points which are:

1. The main functionalities of Smart arbitration in cybersecurity: predict future intrusion threats-detection time- reduction-solving efficiency
2. The technical and/qualitative challenges of Smart arbitration in cybersecurity:
  - The challenges overcome by the system, where:
  - The trust in AI decisions
  - Breaching the system (Data in-Data output)
  - The practical challenges in Developing this systems include:
  - Parity technical systems
  - Economic systems

---

<sup>15</sup> Lamia Tala, Cyber Threats and Crimes: Their Impact on National Security and Strategies to Combat Them, Ma'alam Journal of Legal and Political Studies, University Center of Tindouf, Vol. 84, Issue 82, 2021, p. 6168.

<sup>16</sup> 1. Oxford Dictionary, available at:

[<http://en.oxforddictionaries.com/definition/cyber>](<http://en.oxforddictionaries.com/definition/cyber>)

<sup>17</sup> Idris Atiyah, The Status of Cybersecurity in the Algerian National Security System, Misdakia Journal, University of Al-Arab Tebessa, Vol. 81, Issue 81, 2019, p. 188.

### II. 1-Main Functions of Smart Arbitration in Cybersecurity

According to information from cybersecurity development, special asset lies on smart arbitration in cybersecurity. In this part, we will show you the function of smart arbitration which increases cybersecurity.

#### II.1.1- Transition from Paper-Based to Digital Systems

Smart arbitration is important. First, it plays a crucial role in the creation of paperless arbitration bodies or the transformation from paper-systems of arbitration to electronic systems; that is in the reduction or absence of paper documents in arbitration procedures. The other features in this system are the exchange of documents relating to the dispute as well as the easy handling of arbitration procedures that facilitates the fast resolution of disputes and the improvement of arbitration services.<sup>18</sup>

#### II.1.2- Predicting Future Threats

While there are massive quantities of data passing through the massive institutional networks today, predicting future challenges remains difficult. However, with smart arbitration of this data, future harmful or threatening activities will be quickly identified and substituted. Given the capacities of smart arbitration to process the large sets of information dynamically and in real time, it will be much easier to anticipate and swiftly act upon any threat, or even engineer self-healing solutions to pre-emptively terminate any infectious or harmful activities. This, in turn, will enhance the vigilance of agents and organizations in meting out justice to emergent threats – or what could be called ‘predictive justice’.<sup>19</sup>

#### II.1.3- Speed in Detecting Threats

The ability to detect threats quickly is critical, with 42% of organizations reporting an increase in threats that require rapid detection. Since humans are often slow to analyze the vast amounts of data, smart arbitration becomes the optimal choice. It can scan and analyze large datasets in a short period to identify cyber threats, thereby enhancing cybersecurity. According to statistics, 56% of organizations feel overwhelmed by the sheer volume of threats they face, while 23% report that they cannot effectively handle the identified threats.<sup>20</sup>

### II.2- Challenges of Smart Arbitration in Cybersecurity

If we regard smart arbitration as a model of ADR seeks to resolve the dispute by utilizing the artificial intelligence technologies in lieu to the traditional judiciary system, we can identify a series of challenges that such innovative model can face, in particular the cyber security concerns. The main challenges are:

---

<sup>18</sup> Souad Aghanime, A Study of the Moroccan Experience in Electronic Litigation in Light of Comparative Experiences, *Al-Manara Journal of Legal and Administrative Studies*, Special Issue on the Corona Pandemic, July 2020, p. 275.

<sup>19</sup> Mamdouh Abdel Hamid Abdel Muttalib, *Artificial Intelligence Algorithms and Law Enforcement*, First Edition, Dar Al-Nahda Al-Arabiya, Cairo, 2020, p. 52.

<sup>20</sup> Christopher Rigano, Using Artificial Intelligence to Address Criminal Justice Needs, *NIJ Journal*, National Institute of Justice, Issue No. 280, January 2019, p. 03.

### II.2.1-Technical and Legal Challenges

- **Trust in AI-Based Decisions**

It relates to the concept of smart arbitration as a superior system of arbitration wherein the entire procedure of proceedings concerning the submission of a dispute all the way to the execution of the ruling is carried out by means of smart applications being utilised in a standardised manner by arbitration bodies in special networks that are secure and dedicated to their use. Moreover, the files would be stored in specialised electronic records identified for that purpose, and a ruling would be issued electronically by means of database(s) and intelligent analysis leading to award with execution thereof being automatic according to a set of relevant stipulations – a ruling to be executed according to qualifying regulations. In order to be fair, however, impartiality has to be maintained to leave no room for any algorithmic inherent bias.<sup>21</sup>

- **Privacy and Data Protection**

In cybersecurity arbitration, there will also often need to be access to sensitive or confidential data, which means responsible smart systems need to take measures that ensure data stays protected from misuse or leakage. Smart arbitration must also be capable of conforming to data-protection legislation such as the European General Data Protection Regulation (GDPR),<sup>22</sup> which imposes strict standards on the storage and use of personal data to ensure legal compliance.

- **Algorithmic Bias**

Smart systems rely on available data to learn patterns and make decisions, and if this data contains racial, social, or commercial biases, it may lead to unfair arbitration decisions. To ensure fairness, these systems must be trained on diverse data that fairly represents all parties and scenarios, contributing to objective Smart systems rely on available data to learn patterns and make decisions, and if this data contains racial, social, or commercial biases, it may lead to unfair arbitration decisions. To ensure fairness, these systems must be trained on diverse data that fairly represents all parties and scenarios, contributing to objective and unbiased decision-making.

---

<sup>21</sup> Abdullah Mohamed Ali Salman Al-Marzouqi, E-Litigation and Smart Litigation: A Comparative Study of UAE Legislation with Some Arab and Foreign Systems, *Journal of Legal Sciences*, Sharjah University, Vol. 18, Issue 2, 2021, pp. 249-250.

<sup>22</sup> In 2016, Europe established the “General Data Protection Regulation (GDPR)”, which is responsible for protecting data and privacy for all individuals within the European Union. The GDPR aims to empower citizens to control their personal data and simplify the regulatory and legal framework for international companies by harmonizing laws within the EU. This is a binding regulatory system applied directly without requiring additional legislation from individual countries.

The GDPR protects personal identity information such as names, social security numbers, location data, and online identifiers, along with other factors related to civil, physiological, genetic, mental, economic, cultural, or social identity. It aims to give individuals full control over their personal data and prohibits any entity from accessing this data without their consent. Protected personal data under the regulation includes information like nationality, racial origin, sexual orientation, and health status.

The regulation allows individuals to request the deletion of their stored data, except in cases involving financial obligations, according to Article 17. Individuals also have the right to know what data is stored about them, and it can only be used with their consent. Although designed to protect EU citizens, the GDPR significantly impacts internet users worldwide, as any business processing or collecting data from EU citizens must comply with the regulation, regardless of its location.

### II.2.2- Practical Challenges

- **The Rapid Evolution of Cyber Disputes**

Cybersecurity disputes are fast-evolving, with attack and defense methods continually advancing, and mandating the need for smart arbitration systems that dynamically and flexibly deal with new or novel disputes. As a result, they must regularly enhanced with the latest advancements in cybersecurity – and instructed in how to resolve cross-border disputes as new data emerges.

- **Legal and Ethical Challenges**

There must be clear and unequivocal rules on whether and how smart systems can act legally in making such decisions (including the possibility of challenging such decisions) as a basis for using AI technologies in dispute resolution, since under current legal systems AI-generated legal products remain a legal non-entity. Similarly, there are ethical concerns surround the use of AI in dispute resolution, which are related to the arbitrariness of allowing nonDECT (nonhumans) to make important decisions that potentially impact an actor's outcomes in life or in business..

- **Human-Machine Interaction**

By doing so, at least some level of interaction or conversation between the human arbitrators and the smart systems is required to guarantee the quality of decisions. Thus, while the smart system may make recommendations or provide analyses, the final decision might rely on the judgment of a human being because of moral or human factors. Additionally, according to Alexis Zamyatine, a law student at the Letchworth-based Global University, smart systems should provide communication with the parties in dispute in simple and understandable language in order to facilitate the process of arbitration, and make it even more effective.<sup>23</sup>

- **Flexibility in Arbitration Processes**

Complex Disputes: There are some cybersecurity disputes in which the legal issues are complex and may involve complicated technical and commercial facts. In such cases, smart systems need to make decisions that require the ability to understand the intricacies of the case, and properly analyse the complex evidence.

- **Cost and Implementation**

Although smart arbitration can be more efficient than traditional arbitration, developing AI systems capable of resolving disputes requires significant investments in technology and infrastructure. Moreover, these systems may not be equally available to all disputing parties, especially in developing countries or among small businesses that lack the resources to access advanced technologies.

While smart arbitration speeds up dispute resolution without the need for traditional courts or arbitration, achieving this goal requires overcoming challenges related to trust, privacy, algorithmic biases, and legal regulations.

---

<sup>23</sup> [<https://www.court.chat/index.html>](<https://www.court.chat/index.html>)

## **Conclusion:**

Like many modern technologies, smart arbitration has important virtues, and is arguably faster, more efficient, and technically more secure than traditional arbitration. But when it comes to cybersecurity, its use poses important new challenges, like trust in the decisions of the artificial intelligence, safety of the data, and algorithmic biases.

In this way, this experiment shows that smart arbitration has the potential to resolve disagreements in new ways, and to protect the results of its efforts in novel and effective ways, but also that will come with its own set of dangers. As with renewable energy, we will need to get better at these systems if we want to join the energy revolution without sacrificing fundamental human rights. That will require finding a way to work together in developing the appropriate law, in establishing the appropriate norms of transparency and fairness in how they operate.

Moreover, to address them, we require virtues such as integrity and openness, and we need to ensure that smart systems are updated regularly to keep up with emerging changes made possible by new advances in cybersecurity.

## **Recommendations:**

### **1. Increase Transparency in Smart Arbitration Procedures:**

For companies who use smart arbitration, the training processes and underlying data sets – how they were restricted or channeled to create the algorithms – need to be openly explained and understood by the public. Every ruling needs to be defended transparently. A society that acknowledges algorithmic harms and biases will experience dismay if penalties are imposed upon individuals. A sufficiently technical system can then rescale it and make everyone better. Whereas, given our present ignorance of such systems, it behooves us to stay our hands before they reach any great magnitude.

### **2. Enact National and International Legislation:**

In addition, smart arbitration should be regulated by law in each country to ensure clear-cut legal rules that limit algorithmic biases, better protect privacy and confidentiality, and provide safer channels of appeal against the outcome. International cooperation is essential to create binding agreements on the use of smart arbitration that ensure globally agreed fairness standards.

### **3. Algerian Legislative Framework:**

In this regard, the Algerian legislator must consolidate clearly the body of legislation best suited to address these conflicts generated by technological development. And it is in the context of e-litigation or smart arbitration that they choose the line to follow. It is for this reason that the organization of the Algerian justice and the legal implementation of e-litigation must incorporate the same successive phases of application to the short, medium and long terms.

### **4. Training Programs:**

## **Smart Arbitration in the Service of Cybersecurity**

Training courses should also be held for the judges, their assistants, staff, lawyers and other persons concerned with the arbitration organ to enable them to qualify for the e-courts and electronic arbitration.

### **5. Improve the Quality of Data Used:**

Diversity and fair representation in the data from which smart systems are trained, and regularly monitored and analysed, will minimise the potential for bias in smart decision-making.

### **6. Raise Public Awareness of Smart Arbitration:**

Popular awareness campaigns and workshops should be organized to explain to the public what ‘smart arbitration’ entails, the risks as well as potential benefits, and how to manage its outcomes.

### **7. Effective Monitoring of Smart Systems:**

National institutions and regulatory bodies need to create a mechanism to periodically review arbitration decisions: smart and otherwise — and to ensure that these systems stay within the proper ethical and legal boundaries.

### **8. Amend Arbitration Laws to Accommodate Technological Advancements:**

Existing arbitration laws can be amended to incorporate technological law developments, rules and mechanisms for mitigating data breaches relating to the dispute, and specialized laws can be passed to explicitly cover all issues touching upon any smart arbitration dispute, be it related to electronic transactions, smart arbitration and otherwise.

9. Clarify Rules for International Jurisdiction:

More generally, rules of international jurisdiction for courts could be further developed at the national and at treaty levels, and guidelines developed for the recognition of rulings by smart arbitral bodies.

### **10. Encourage Dialogue Between Various Stakeholders:**

Give governments, companies and civil organizations access to smart contracts to double-check their compliance with individual rights and other needs. In addition to the use of smart arbitration technologies, international law should regularly update the systems to keep pace with technological developments.

### **11. Strengthen Cybersecurity Measures:**

On individual level, computer security system must be used in institutions, at the same time, we can also use AI technologies to improve cyber-security's level, meanwhile, more strategies must be used and security team must be trained to use these technologies.