Revista Jurídica unicuritiba

Submetido em: 23/08/2024
Aprovado em: 15/09/2025
Avaliação: Double Blind Reviewe
ISSN: **2316-753X**

JUDGMENTS AND ARGUMENTS IN THE FIELD OF CYBERSECURITY IN JORDAN: FROM SCIENCE FICTION TO FUTURE REALITIES

JULGAMENTOS E ARGUMENTOS NO DOMÍNIO DA CIBERSEGURANÇA NA JORDÂNIA: DA FICÇÃO CIENTÍFICA ÀS REALIDADES FUTURAS

MONTHER ABDEL KARIM AHMED AL-QUDAH
Department of Private Law, Faculty of Law, Amman Arab University, Jordan
m.alkodah@aau.edu.jo
https://orcid.org/0000-0001-5773-8792

INAS AL KHALDI
Amman Arab University, Jordan
i.alkhaldi@aau@edu.jo
https://orcid.org/0000-0003-3759-0924

MOHAMMAD HUSSEIN MOHAMMAD AL-AHMAD
Amman Arab University, Jordan
m.alahmad@aau.edu.jo
https://orcid.org/0000-0003-2009-7535

MOHAMMAD ASSAF ALSALAMAT
Amman Arab university, Department of Private Law, Jordan
h.shakhatreh@jadara.edu.jo
https://orcid.org/0009-0003-8744-6995

HISHAM JADALLAH MANSOUR SHAKHATREH
Jadara university, Jordan
h.shakhatreh@jadara.edu.jo
https://orcid.org/0000-0001-8693-5744

NASIR ALBALAWEE
Jadara University, Jordan
nbalawi@jadara.edu.jo
https://orcid.org/0000-0001-9497-3572

ABSTRACT

Because of the speed at which technology is developing, cyberspace has changed dramatically, and users now handle enormous volumes of sensitive data on a regular

Submetido em: 23/08/2024
Aprovado em: 15/09/2025
Avaliação: Double Blind Reviewe
ISSN: **2316-753X**

basis. But this development has been accompanied by a range of challenges, including a growing number of disputes such as information theft and attempts to breach the security of computers, networks, programs, and data. These increasing challenges call for faster and more efficient methods of resolution. Arbitration emerges as a practical and cost-effective tool that can effectively address these issues. Even though cybersecurity issues are inherently complex, arbitration offers a strong and adaptable framework to help resolve them. This paper examines the challenges faced in Jordan within this dynamic domain, emphasizing Arbitration as the most viable approach to dispute resolution. It delves into critical aspects of cybersecurity, including data breaches, supply chain attacks, and adherence to national and international cybersecurity laws, after which the usefulness of arbitration in resolving conflicts in these domains is examined. Additionally, the paper discusses cybersecurity-related issues specific to Jordan while evaluating how Arbitration can contribute to their resolution. Additionally, it makes suggestions for enhancing dispute resolution procedures through targeted initiatives include procedural innovations, stakeholder participation, capacity building, and legislative framework reforms. These recommendations should make arbitration a more adaptable and effective way to resolve cybersecurity disputes in Jordan.

Keywords: Arbitration; Cyber security; Data breaches; Dispute resolution; Supply chain attacks.

RESUMO

Devido à velocidade com que a tecnologia está se desenvolvendo, o ciberespaço mudou drasticamente e os usuários agora lidam com enormes volumes de dados confidenciais regularmente. Mas esse desenvolvimento foi acompanhado por uma série de desafios, incluindo um número crescente de disputas, como roubo de informações e tentativas de violar a segurança de computadores, redes, programas e dados. Esses desafios crescentes exigem métodos de resolução mais rápidos e eficientes. A arbitragem surge como uma ferramenta prática e econômica que pode efetivamente abordar essas questões. Mesmo que os problemas de segurança cibernética sejam inerentemente complexos, a arbitragem oferece uma estrutura forte e adaptável para ajudar a resolvê-los. Este artigo examina os desafios enfrentados na Jordânia dentro deste domínio dinâmico, enfatizando a arbitragem como a abordagem mais viável para a resolução de disputas. Ele investiga aspectos críticos da segurança cibernética, incluindo violações de dados, ataques à cadeia de suprimentos e adesão às leis nacionais e internacionais de segurança cibernética, após o que a utilidade da Arbitragem na resolução de conflitos nesses domínios é examinada. Além disso, o documento discute questões relacionadas à segurança cibernética específicas da Jordânia, enquanto avalia como a arbitragem pode contribuir para sua resolução. Além disso, faz sugestões para aprimorar os procedimentos de resolução de disputas por meio de iniciativas direcionadas, incluindo inovações processuais, participação das partes interessadas, capacitação e reformas da estrutura legislativa. Essas recomendações devem tornar a arbitragem uma maneira mais adaptável e eficaz de resolver disputas de segurança cibernética na Jordânia.

Palavras-chave: Arbitragem; Segurança Cibernética; violações de dados; resolução de disputas; ataques à cadeia de suprimentos.

Submetido em: 23/08/2024
Aprovado em: 15/09/2025
Avaliação: Double Blind Reviewe
ISSN: **2316-753X**

1 INTRODUCTION

The rapid growth and widespread adoption of cyberspace, fueled by emerging technologies, have brought about new risks that threaten individuals, businesses, national infrastructure, and governments alike (Reveron, 2012). In Jordan, the cybersecurity landscape is progressing, supported by comprehensive laws designed to safeguard data and address cybercrime. Arbitration has concurrently become a critical mechanism for resolving disputes in the realm of cybersecurity, backed by strong legislation and institutions fostering international collaboration. Jordan has made notable progress in strengthening its cybersecurity framework, particularly through legislative efforts to counteract cybercrime and ensure data protection (Ghandour & Woodford, 2024). Among these efforts is the enactment of the Cybercrimes Law No. (17) of 2023 is the primary legislation that governs cybersecurity breaches in Jordan. It criminalizes various outlawed activities, such as unauthorized access, interception, and interference with computer systems and data. This Law is complemented by Personal Data Protection Law No. 24 of 2023; This establishes a legal framework for the protection of personal information in Jordan. It establishes the rights and obligations of data controllers and data subjects, as well as the protocols for handling data breaches (AL-Billeh, 2024). The Data Protection Law imposes strict standards on data controllers and processors to ensure the security of personal data, including measures to prevent unlawful data loss, alteration, or destruction (Magableh, 2024).

The interplay between arbitration and cybersecurity is increasingly relevant, particularly as disputes involving technology and data breaches are on the arise. Jordan 's commitment to international arbitration is underscored by its membership in the Since 1979, the New York Convention has made it easier for international arbitral awards to be recognized and enforced. In accordance with the UNCITRAL Model Law, the Arbitration Law of 2018 regulates both local and international arbitration, guaranteeing uniformity and conformity to international norms.

The question of cybersecurity assumes special importance in an international arbitration setting. Data breaches have been a huge threat in Jordan, just like in other parts of the world at large, to companies, governments, and individuals (Al-Kasassbeh and Ghazleh, 2023). Other than intrinsic cybersecurity risks that all parties associated with international arbitration processes are exposed to, the possibility of data loss or

Submetido em: 23/08/2024
Aprovado em: 15/09/2025
Avaliação: Double Blind Reviewe
ISSN: **2316-753X**

breach is increased when they must communicate information in order to settle a disagreement (Rao, 2024). These include unauthorized access to data systems, which results in information loss, theft, or alteration. The main legislation governing data protection and privacy in Jordan is found in Data Protection Law, No. (24) of 2023, which draws inspiration from the European Union's ("EU") General Data Protection Regulation ("GDPR") became operative in May 2018. The foundation for understanding the legal requirements and the potential conflicts arising from infractions is laid by this background.

National required regulations that vary greatly from state to state regulate cybersecurity and the privacy of personal data. These concerns are not specifically addressed by any of the mandatory clauses in the arbitration rules or national arbitration laws. Such limitations on personal data could be relied on to object to the production of some required documents or to their being submitted as evidence in the arbitral procedure (Anderson and Verbist, 2024). As a result, their application to the handling of evidence is very limited. It is also important procedurally in that the safeguarding of personal information is dependent on the safeguarding of system operation and integrity. On a technical level, it is also important to protect the secrecy of communications that are between arbitrators or within one party's system to avoid a conflict of interests and factual discrepancies between the parties (Mwangi & Otieno, 2024). Equally important is that any digital evidence that will be produced be preserved and its authenticity maintained throughout the legal process.

Arbitration needs to be set up and run in a fashion guaranteeing adherence by all parties to it, as it's not exempt from these laws (Anderson and Verbist, 2024). Arbitrarily operated institutions may have a unique ability to deal with cybersecurity threats reliably and on a long-term basis. By doing so, such arbitral institutions may well be better placed to differentiate their services, which are already uniquely well-placed to innovate—from the competition and to attract

"Cybersecurity-conscious" clients by way of example for their creativity, at the same time as promoting the institution arbitration as opposed to ad hoc arbitration (Cybersecurity in International Arbitration, 2024).

2 UNPACKING THE DATA BREACHES IN CYBERSECURITY

Submetido em: 23/08/2024
Aprovado em: 15/09/2025
Avaliação: Double Blind Reviewe
ISSN: **2316-753X**

A personal data breach, as defined by the Data Protection Law, No. (24) of 2023, is any security event that causes personal data being communicated, stored, or processed in any other way to be accidentally or unlawfully destroyed, lost, altered, disclosed, or accessed. Therefore, it doesn't have to be unlawful or unauthorized, like in the instance of a hacker; it can even be the consequence of something as straightforward as an employee inadvertently disclosing information to the public. To determine if a data breach has occurred, the Data Protection Act outlines two crucial components. First, there is a genuine danger of harm to the data subject whose personal data was accessed without authorization; second, personal data should not have been accessed by an unauthorized person.

Under the Data Protection 2021 Regulations, a breach can be harmful when it involves the data subject's full name or an identification number (Admissibility of Illegally Obtained Evidence in International Arbitration BY ACERIS LAW LLC, 2024). Under the Data Protection Regulations 2021, data In the case of a breach, subjects' financial information—such as bank account numbers, credit or debit card details, health-related information, and income information—such as salaries, bonuses, or money received from the sale of commodities or property—may be considered harmful. An exception would be information that is published by law or that is, thus, in the public domain. However, a data breach cannot expose such information to the public.

In any adjudicatory hearing, the cardinal values of honesty, fairness, and due process are infringed when one party or both parties present illegally obtained evidence. It may bring about financial and public relations damage to corporations, governments, lawyers, and other institutions whose records were accessed or whose negligence was apparent. Moreover, liability and regulatory fines under relevant privacy regimes may arise in case of a personal data breach. Of more importance, however, any failure of cybersecurity necessarily damages the legitimacy and credibility of international arbitration as a means of resolving disputes as the procedure is inherently secret. There are key factors as to why hackers might be driven to hack international arbitrations. First and foremost, international arbitration provides for a neutral forum on the resolution of business and investment disputes. Parties to international arbitration are often victims of cyber-attacks, which have included international corporations, governments, public figures, state institutions, and NGOs. The second reason is that it enables the confidential resolution of disputes, even

Submetido em: 23/08/2024
Aprovado em: 15/09/2025
Avaliação: Double Blind Reviewe
ISSN: **2316-753X**

though the degree and extent of confidentiality differ. International arbitration cases typically involve the disclosure of documents regarding facts not generally known to the public that could impact the political and financial systems of various corporations.

Thirdly, parties in different countries are based in a variety of contexts when conducting international arbitration. Parties are usually represented by sizable, frequently international teams.

The issue of data breaching has also affected various law firms, noting that most store their data in open clouds and there is no encryption of messages between the arbitrators and their clients in most of the interactions. In a recent survey of 200 law firms by the cybersecurity consulting firm Logic force all of the respondents reported having been targeted by hacking. What was most astonishing is that they were not aware of the breaches until the survey brought the issues to light and relevant actions were taken.

These incidents have occurred in arbitral processes as well as in legal offices. Turkey admitted in the Libananco v. Republic of Turkey lawsuit that it had intercepted communications between Libanan and its legal representatives as well as other correspondence pertaining to albeita as part of a larger criminal investigation (Kurban et al., 2015). Even with their resources and exposure, law firms are still not sufficiently equipped to handle these risks. 40% of companies were genuinely ignorant of the attempts at hacking, according to a Logic Force survey conducted prior to the research and associated investigations. Additionally, just 23% of companies had a sufficient cyber-attack insurance policy in place, and 95% of companies either did not fully follow or comply with their own data governance and cybersecurity rules.

Cyber weaknesses, which are prevalent in the storage of sensitive information with regard to reputation management and regulatory compliance and are changing over time, are particularly easy to target arbitral institutions. In July 2015, during the hearing on the maritime border dispute between China and the Philippines, the Permanent Court of Arbitration in The Hague experienced a website hack. 18 The PCA website had malware installed, which put users' computers at danger of data theft. Additionally, In the case of Caratube v Kazakhstan19, also in the same year, Eventually, the claimant obtained some documents that had been released from the incident in which the Kazakh government's IT system's private information was exposed (Akhmetov et al., 2018). The tribunal allowed the claimant to introduce non-privileged documents from the leak that resulted from the information, even though it

Submetido em: 23/08/2024
Aprovado em: 15/09/2025
Avaliação: Double Blind Reviewe
ISSN: **2316-753X**

was obtained through hacking. This was because there was no rule or regulation that prevented the tribunal from using its discretion to admit evidence that was obtained in this way. There is also anecdotal evidence of arbitrations in which case database compromise or release has occurred exposures that would not have arisen had the appropriate security measures been implemented.

These dangers highlight the importance of considering Data Protection during an arbitration process. Thankfully, a host of tools are now available to parties and arbitrators. Despite these risks inherent in this modern threat, many arbitration institutions still rely on fairly insecure means of communication and storage technology. These risks to which arbitral institutions are exposed may be best evidenced by the attacks on the PCA. The possibility exists that, during an arbitration, the parties will need to disclose private information to substantiate their claims. Even though, in most jurisdictions, it is taken for granted that the process of arbitration will occur behind closed doors, cyberattacks present a great threat to the confidentiality of the process.

3 INTERNATIONAL ARBITRATION MEASURES TAKEN TO COUNTER THE EFFECT OF DATA BREACHES IN CYBER SECURITY

However, the arbitral community has responded to this challenge in a number of ways. The arbitration community has placed a great deal of emphasis on data protection because of the rise in cyberattacks in recent years. The majority of respondents to a 2018 Queen Mary University survey stated that arbitration rules ought to include the safety of electronic data and communications. Last year, the New York City Bar Association, the CPR Institute, and the ICCA published the Cyber Security Protocol for International Arbitration. is arguably the most notable example. On September 19, 2022, the Working Group unveiled the 2022 Edition of its Protocol during the ICCA Congress in Edinburgh. After taking into account the opinions of the parties, the tribunal is empowered by the Protocol to decide which security measures are suitable given the circumstances. It is obvious that any such protocols must cover a wide range of topics, including data security, information storage, and the transmission and communication of material between the arbitrators and their

Submetido em: 23/08/2024
Aprovado em: 15/09/2025
Avaliação: Double Blind Reviewe
ISSN: **2316-753X**

personnel. Crucially, the Protocol stipulates that all parties to an arbitration have a shared responsibility for cybersecurity and that each party must make sure all arbitration staff members are informed of and abide by any cybersecurity measures implemented. The creation of an ICCA-IBA Joint Task Force on Data Protection in International Arbitration has also been assigned the responsibility of creating a guidebook that would help with the possible effects of data protection regulations, particularly the GDPR.

Furthermore, the problem of cyberattacks is being addressed institutionally by arbitral institutions themselves. "Any secured online repository that the parties have agreed to use" is recognized as a communication channel under the HKIAC Rules, which were revised on November 1, 2018. Article 30A lays out new rules for cybersecurity and data protection, while Article 24A lays out compliance measures concerning money laundering, tax evasion, fraud, bribery, corruption, financing of terrorism, and trade or economic penalties. Last but not least, on October 1, 2020, the LCIA will implement the revised Arbitration Rules. The incorporation of arbitration into the global cybersecurity framework is essential as the cybersecurity environment continues to change. A dedication to embracing arbitration as a crucial dispute resolution process for cyber security conflicts is demonstrated by the development of procedures and the proactive reaction of arbitral institutions. The International Arbitral community guarantees that arbitration will continue to be a practical and reliable means of settling complicated disputes in the digital era by giving arbitration top priority in cybersecurity.

4 CHALLENGES IN PROTECTING THE CYBERSECURITY SPACE IN JORDAN

Cybersecurity protection in Jordan faces a number of issues. These issues include Rapid technological changes which, as stated, are hugging the world at a rather high speed. With these comes a dimension of change whose pace is faster than the ability for appropriate legal and regulatory frameworks to keep up. An example is the regime on cyber security: with incidents of cyber-attacks in Jordan, and indeed nearly all other countries, legal regimes tend to be too slow to catch up with new challenges, therefore creating protection gaps or remedial mechanisms. 51% of firms are increasing their investments in cyber security because, according to the 2023 IBM

Submetido em: 23/08/2024
Aprovado em: 15/09/2025
Avaliação: Double Blind Reviewe
ISSN: **2316-753X**

Cost of Data Breach Report, the average cost of data breaches worldwide rose by 15% from 2020 to USD 4.45 million. There has been a significant spike in cyber-attacks within Jordan; more than 2455 occurrences have been reported in the past one year.

Additionally, in most cybersecurity disputes, evidence is complex and technical in nature, and the traditional courts might not be prepared for the same. This can refer to digital forensic evidence, logs, and highly technical testimonies regarding the nature of cyberattacks and data breaches. Thus, often the most common material that is subject to a possible cyber-security dispute is of a sensitive nature, which the parties may not want publicly disclosed, such as trade secrets, intellectual property, and details of security breaches that, if revealed in open court, might adversely affect a company's reputation or cause further security vulnerabilities. It is essential that issues are resolved quickly as Cyber security incidents do damage that can escalate very fast; therefore, it needs quick and decisive action that will mitigate harm (Aksoy, 2024). Traditional legal proceedings can take years, while timely resolution of disputes is crucial in the context of cybersecurity to cease further or future damage.

5 ADVANTAGES OF ARBITRATION IN CYBERSECURITY

It is for this reason that arbitration becomes advantageous to most as its capacity for solving the cybersecurity issues, although not quite developed to fully curb the issues, it still does play an influential role. The ability to appoint arbitrators with specialized subject matter expertise in areas such as cybersecurity in which they will be better placed to understand complex technical evidence and issues at stake may go on to create more informed, and hence accurate, decisions than those achieved through traditional courts by generalist judges. Moreover, the private nature of the arbitration procedures helps in keeping sensitive information confidential and hence out of the public eye, which is very imperative for addressing confidentiality concerns in disputes related to cybersecurity (Brown, 2021). This can be paramount for a company wishing to maintain its reputation and safeguard against further cyber-attacks.

Arbitration procedures can also be customized to meet the interests of the parties involved by implementing faster dispute settlement timetables, among other things. In order to lessen the damage caused by a cybersecurity disaster, this latter

Submetido em: 23/08/2024
Aprovado em: 15/09/2025
Avaliação: Double Blind Reviewe
ISSN: **2316-753X**

flexibility is crucial. This adaptability also makes it possible for the award to be easily enforced anywhere in the world, which is arbitration's further advantages in cybersecurity. Compared to court decisions, the New York Convention on the Recognition and Enforcement of Foreign Arbitral results significantly simplifies the process of enforcing arbitration results overseas. This is especially important in conflicts involving cyber security, which frequently involve worldwide parties. Arbitration rules can be chosen by the disputing parties if they believe they are fair and predictable, and they can also specify how impartial experts will be appointed. Parties handling the high stakes of cybersecurity incidents may find solace in this predictability.

6 CONCLUSION

In conclusion, considering that the disputes concerning cybersecurity in Jordan present problems unique to them, such as specialized knowledge, issues of confidentiality, complexity of evidence, issues that are transboundary, and the need for timely resolution, arbitration proves efficient and effective in dispute resolution. Such advocacy on the general adoption of arbitration for this area may be quite effective at mitigating the effects of a cybersecurity incident, much better than traditional litigation could do, so that entities in Kenya can confidently and securely navigate these turbulent waters of cyber threats.

For arbitration to have a solid footing in the resolution of cases on cybersecurity in Jordan, a multifaceted approach is required. Even though specialized knowledge and flexibility in procedure make arbitration a more tenable dispute resolution mechanism to adapt to challenges presented by disputes related to cybersecurity, while affording enhanced measures of confidentiality, further development in this area encompasses the need to standardize practices, increase training, cooperation across borders, specific consideration of cybersecurity by arbitration agreements, and improved security measures. It is this kind of evolution that will further cement the effectiveness and attractiveness of arbitration as a method of resolving intricate cybersecurity conflicts both domestically and abroad.

Submetido em: 23/08/2024
Aprovado em: 15/09/2025
Avaliação: Double Blind Reviewe
ISSN: **2316-753X**

7 RECOMMENDATIONS

To effectively align arbitration with the challenges posed by data breaches under the Jordanian Data Protection Law, 2023, and to ensure it acts as a practical means of resolving disputes in the current digital era, a number of significant advancements are required. These should try to improve the structure that arbitration uses, making sure it is strong, adaptable, and capable of managing the subtleties of disputes involving cyberspace. Arbitration as a means of dispute resolution confers numerous benefits in dispute resolution, including cybersecurity-related disputes, through the provision of a more confidential, flexible, and quicker process compared with traditional court litigation. Considering the specificity and complexity of cybersecurity disputes, further adjustments and evolution of arbitration practices are necessary. This is not only relevant in Jordan but all over the world, since the cyber threats do not respect borders. By developing a method to gather data that cannot be gathered through existing legal channels, Jordan can counter the danger to cybersecurity. Some of the simplest measures that can be done in this regard are forced logouts, automated password management with secondary authentication, and restricting access when the computer or terminal is left unattended for a short while. Firewalls, nested access rights systems, and other port-protecting software that immunizes the system are additional easy measures. highly advanced artificial intelligence-based monitoring software that can track suspicious activity within the directory structure. Furthermore, transparent technologies that operate in the background for authorized users can encrypt the data. To ensure that they can access the system and utilize it properly, all users should also be required to complete a training session. Some insurance companies that offer coverage for cyber security breaches also offer assistance in creating and putting these strategies into action.

Jordan could look into providing legislation that expressly provides for Cybersecurity Dispute Arbitration. While the Arbitration Act provides a general framework relating to arbitration, what is still needed are some specific provisions that take into consideration the peculiarity of the issues in regard to the disputes relating to cyber security. This has included: detailed procedures for the handling of digital evidence, timelines sensitive to the urgency of addressing cyber incidents, and provisions for virtual hearings, in particular, with regard to cyber disputes. These legislations could also include provisions that set up specialized arbitration centers that

Submetido em: 23/08/2024
Aprovado em: 15/09/2025
Avaliação: Double Blind Reviewe
ISSN: **2316-753X**

expressly deal with cyber-dispute resolution. Such specialized arbitration centers on cyber-dispute resolution could be beneficial in Jordan. For example, institutions have to avail lists of arbitrators well-versed in cyber law, data protection, and information technology to ensure that complex technical issues at the very heart of data breach disputes are not only appreciated but also effectively adjudicated.

The provisions could include very specific cyber-arbitration protocols that enable them to deal with the arbitration issues. There is a requirement to set arbitral procedures tailor-made for cyber disputes. The process of conducting arbitration would mean emphasis on confidentiality and data security, the extent to which digital evidence is presented, and rules for assessing damages in the event of data leakage. Further, it can specify the qualifications an arbitrator is required to have to take up such disputes, indicating exposure to requisite skills in matters concerning cyber law and related principles with data protection.

One more practical step in this respect would be to include arbitration clauses in IT contracts, such as those related to cloud services, data processing, and software development, in scenarios arising from the landscape of data breaches. These clauses will have to spell clearly that the dispute resolution method of choice is arbitration, state which rules shall apply while conducting the arbitral procedure, and establish beforehand the parties' acceptance of the jurisdiction of the arbitrators and the choice of law.

Most importantly, convincing stakeholders of the feasibility of arbitration to handle data breach disputes will call for clear awareness of coinage among businesses, government institutions, and legal professionals. Capacity-building in training programs and workshops regarding arbitration over cyber security is quite important. They can help in demystifying the arbitration procedure and provide benefits that come out when handling disputes of this nature. Since data breaches are a cross-border issue, Jordan has to seek harmony in its approach of arbitration in Cyber Security disputes through inclusion of international practices and principles. This may borrow best practice from jurisdictions which have an advanced cyber-arbitration framework and be present in international forums addressing issues of cyber dispute resolution. This collaboration will help improve the efficiency and enforceability of the arbitral award across jurisdictions.

Submetido em: 23/08/2024
Aprovado em: 15/09/2025
Avaliação: Double Blind Reviewe
ISSN: **2316-753X**

REFERENCES

Admissibility of Illegally Obtained Evidence in International Arbitration BY ACERIS LAW LLC. https://www.acerislaw.com/admissibility-of-illegally-obtained-evidence-in-international-arbitration/ Accessed July 14 2024

Akhmetov, A. T., Bekisheva, S. D., Syrbu, A. V., & Kainazarova, D. B. (2018). Retrospective review of information technologies in the Criminal Code of Kazakhstan. Journal of Advanced Research in Law and Economics, 9(35), 1545-1550.

Aksoy, C. (2024). Building a cyber security culture for resilient organizations against cyber attacks. İşletme Ekonomi ve Yönetim Araştırmaları Dergisi, 7(1), 96-110. https://doi.org/10.33416/baybem.1374001

AL-Billeh, T. N. (2024). Legal framework for protecting the right to private life in the digital space: the extent to which Jordanian constitution and legislation takes into account international requirements. Revista de Investigações Constitucionais, 11(1): e258. https://doi.org/10.5380/rinc.v11i1.90631

Al-Kasassbeh, F. Y., & Ghazleh, A. M. A. (2023). International and National Efforts to Protect Cyber Security: Jordan Case Study. International Journal of Cyber Criminology, 17(2), 350-363. https://cybercrimejournal.com/menuscript/index.php/cybercrimejournal/article/view/263

Anderson, A., & Verbist, H. (Eds.). (2024). Expedited International Arbitration: Policies, Rules and Procedures. Kluwer Law International BV.

Brown, J. C. P. (2021). The protection of confidentiality in arbitration: balancing the tensions between commerce and public policy (Doctoral dissertation, London Metropolitan University). https://repository.londonmet.ac.uk/6685/

Cybersecurity In International Arbitration (2024) A Necessity And An Opportunity For Arbitral Institutions By Claire Morel de Westgaver.

Ghandour, A., & Woodford, B. J. (2024). Guidelines to develop a cybersecurity policy in schools, perspectives informed from Jordanian Cybercrime Law. In 2024 25th International Arab Conference on Information Technology (ACIT) (pp. 1-6). IEEE. https://doi.org/10.1109/ACIT62805.2024.10876919

https://arbitrationblog.kluwerarbitration.com/2017/10/06/cyber-security/; accessed on 12th July 2024

Kurban, D., Erözden, O., & Gülalp, H. (2015). Supranational rights litigation, implementation and the domestic impact of Strasbourg Court jurisprudence: A case study of Turkey. Hertie School of Governance. https://opus4.kobv.de/opus4-hsog/frontdoor/index/index/docId/1758

Submetido em: 23/08/2024
Aprovado em: 15/09/2025
Avaliação: Double Blind Reviewe
ISSN: **2316-753X**

Magableh, N. Z. (2024). The Adequacy of the Laws Regulating Electronic Business in Jordan. Public Administration and Law Review, (1 (17)), 66-77. https://doi.org/10.36690/2674-5216-2024-1-66

Managing Data Privacy and Cybersecurity Issues By Erik G W

Mwangi, V. J., & Otieno, H. (2024). Arbitration as a Dispute Resolution Method in the Cybersecurity Space in Kenya: Advancing Towards New Frontiers. Available at SSRN 4958854. https://dx.doi.org/10.2139/ssrn.4958854

Rao, Z. F. (2024). Human-Centric Cybersecurity: Safeguarding Individuals in the Digital Age. https://dspace.cuni.cz/bitstream/handle/20.500.11956/197704/120483475.pdf?sequence=1

Reveron, D. S. (Ed.). (2012). Cyberspace and national security: threats, opportunities, and power in a virtual world. Georgetown University Press.

Schäfer; https://globalarbitrationreview.com/guide/the-guide-evidence-in-international-arbitrati on/2nd-edition/article/managing-data-privacy-and-cybersecurity-issues Accessed July 14 2024

What is GDPR, the EU's new data protection law?https://gdpr.eu/what-is-gdpr/#:~:text=The%20regulation%20was%20put%20into,tens%20of%20millions%20of%20euros . Accessed July 14, 202