

The Role of Mediation and Arbitration in Data Breach Disputes: Balancing Efficiency, Privacy, and Enforcement

Daniyal Shoukat *

Makale Türü/Article Type: Derleme Makalesi/Review Article

Gönderim/Received: 08.01.2026, **Kabul/Accepted:** 20.08.2026, **Yayın/Published:** 30.09.2026

Abstract: The increased popularity of the information leakage has provided an even greater need in the usage of efficient and safe tools of dispute resolution. The traditional litigation has been identified to be ineffective in resolving the complexities of data driven disputes resulting in the adoption of ADR practices. The paper will analyze the possibility of the ADR mechanisms, such as mediation, arbitration, negotiation, expert determination, conciliation, Early Neutral Evaluation, Online Dispute Resolution and ombudsmen services to the resolution of data breach disputes. It deals with mediation as a cooperative flexible approach, in high stakes cybersecurity, and arbitration is considered in the perspective of legal recognition and international enforcement. The benefits of ADR in data breach claims that are critically analyzed are cost-effectiveness, confidentiality, and, the amplified access to justice. Nevertheless, there are also issues associated with it such as the loopholes of the regulation, accessibility, consent-based ethical dilemma, and the boundaries of enforcement. In the paper, the discussion of the practical strategies of implementation proceeds with the emphasis on the necessity of effective legal frameworks, the sequence of the dispute resolution procedures, and the increasing importance of ODR. The article will assist in discussing the aspects of optimizing ADR in data breach cases by providing a summary of the existing literature and defining the areas of research that should be addressed further.

Keywords: Alternative Dispute Resolution (ADR), data breaches, mediation, arbitration, cybersecurity, On-line Dispute Resolution (ODR), cross-border disputes.

* Wakalat Online LLP; Young Mediators Forum Pvt. Ltd.; Department of Law, University of Punjab, Jhelum Campus, Jhelum/Pakistan, e-mail: daniyalshoukat9987@gmail.com, ORCID: 0009-0003-1419-1135

Atıf/Citation: Shoukat, Daniyal. "The Role of Mediation and Arbitration in Data Breach Disputes: Balancing Efficiency, Privacy, and Enforcement". *DiHA: Journal of Interdisciplinary Legal Studies*, no. 3 (2026): 64-76. <https://doi.org/10.5281/zenodo.22958734>



Bu çalışma Creative Atıf-GayriTicari-Türetilemez 4.0 Uluslararası (CC BY-NC-ND 4.0) ile lisanslanmıştır. | This work is licensed under a Creative Commons Attribution-NonCommercial- NoDerivatives 4.0 International (CC BY-NC-ND 4.0).

Veri İhlali Uyuşmazlıklarında Arabuluculuk ve Tahkimin Rolü: Etkinlik, Gizlilik ve İnfazın Dengelenmesi

Öz: Bilgi sızıntılarının artan yaygınlığı, etkin ve güvenli uyuşmazlık çözüm araçlarının kullanımına duyulan ihtiyacı daha da artırmıştır. Geleneksel yargılamanın, veri odaklı uyuşmazlıkların karmaşıklığını çözmede yetersiz kaldığı tespit edilmiş, bu durum Alternatif Uyuşmazlık Çözümü (ADR) uygulamalarının benimsenmesiyle sonuçlanmıştır. Bu makale; arabuluculuk, tahkim, müzakere, uzman belirlemesi, uzlaştırma, Erken Taraflı Değerlendirme, Çevrimiçi Uyuşmazlık Çözümü (ODR) ve ombudsmanlık hizmetleri gibi ADR mekanizmalarının veri ihlali uyuşmazlıklarının çözümündeki uygulanabilirliğini analiz edecektir. Çalışma, arabuluculuğu yüksek riskli siber güvenlik konularında işbirlikçi ve esnek bir yaklaşım olarak ele alırken; tahkimi hukuki tanınırlık ve uluslararası tenfiz perspektifinden değerlendirmektedir. Veri ihlali taleplerinde ADR'nin eleştirel bir gözle analiz edilen faydaları; maliyet etkinliği, gizlilik ve adalete erişimin güçlendirilmesidir. Bununla birlikte, mevzuattaki boşluklar, erişilebilirlik, rızaya dayalı etik ikilemler ve tenfizin sınırları gibi bu yöntemlerle ilişkili sorunlar da mevcuttur. Makalede, uygulamaya yönelik pratik stratejilerin tartışılması; etkin yasal çerçevelerin gerekliliği, uyuşmazlık çözüm prosedürlerinin sıralaması ve ADR'nin artan önemine yapılan vurgu ile sürdürülmektedir. Bu makale, mevcut literatürün bir özetini sunarak ve daha fazla ele alınması gereken araştırma alanlarını tanımlayarak, veri ihlali davalarında ADR'nin optimize edilmesi hususlarının tartışılmasına katkı sağlayacaktır.

Anahtar Kelimeler: Alternatif Uyuşmazlık Çözümü (ADR), veri ihlalleri, arabuluculuk, tahkim, siber güvenlik, Çevrimiçi Uyuşmazlık Çözümü (ODR), sınır ötesi uyuşmazlıklar.

Introduction

Alternative Dispute Resolution (ADR) are the practices that are employed to challenge legal cases without the conventional litigation in a court of law, including mediation, arbitration and negotiation. ADR has already gained much scholarly and practical attention to the specific area of data breach disputes. This added topicality can be explained by the growing pace of the privacy violation trends and the legal concerns they cause to companies worldwide. The data breach scandals tend to be a complicated struggle between the organization which is the victim of the security breach and other groups, such as the victims, business partners, government regulators, and the insurance companies. These conflicts typically center on some of the most noticeable concerns including the payment of damages received, apportionment of the liability among the involved parties, the non-compliance with the regulations, and adherence to the breach notification provisions.

The traditional court system tends to be a counter-efficient approach to dealing with the peculiarities of data breach cases. These are usually highly technical issues, which involve intricate technicalities of cybersecurity and data infrastructure, far-reaching effects to large numbers of individuals, and the dire need of an immediate solution to limit the further harms and regulatory penalties. Consequently, ADR mechanisms emerge as a compelling alternative pathway. The trend is also enhanced by the spread of strict data protection laws, including the General Data Protection Regulation (GDPR) and a range of diverse state-

level privacy laws that have contributed significantly to the number of disputes concerning data, which is supposed to be effectively addressed.

Data breaches are complex and, thus, cause numerous forms of disputes. These include the conflicts between the breached organizations and the aggrieved customers who demand redress, enforcement efforts of the regulatory agencies, contractual disputes on the implication of the breach to the business partners and the widespread and class action lawsuits of the aggrieved. Formal litigation, which is a formal remedy, has very serious drawbacks in this regard; it is in most cases prohibitively expensive, too time-consuming, and outcomes are highly publicized. Reputational losses of organizations may be exacerbated by the fact that the court proceedings take place publicly and will continue to undermine customer loyalty. Such failings have led the ADR methods particularly the mediation and arbitration to reinforce their position as a potential and viable way of resolving data breach disputes. Mediation is voluntary interference of a third party who is an impartial individual to facilitate a mutually agreeable settlement between the disputants. In arbitration though, there is a neutral arbitrator and upon learning the evidence and arguments of both parties, a binding decision is made. Research indicates that the ADR approaches bring special advantages to a data breach case, such as a much quicker resolution time, much less expensive than a lawsuit, much more privacy since no court records can be created, and the possibility of using expert specialists with a clear understanding of the technical and legal issues involved in cybersecurity breach cases.

1. Types of ADR in Data Breach Disputes

ADR is the term used to describe several systematic conflict resolution processes that are unrelated to litigation. ADR offers flexible, efficient, and in most instances, confidential actions in the context of the dispute in the data breach case against the technical and relationship complexity of the cybersecurity breach. The major ADR tools that are used in this field are mediation, arbitration, negotiation, expert determination, conciliation, early neutral evaluation, ODR and the ombudsmen services. All solutions are used in different ways and are chosen depending on the type of conflict, priorities of the parties and the required result.

1.1. Mediation

Mediation is a negotiated process that is assisted by a third party mediator who helps the parties to the conflict find a solution that is acceptable to both of them.¹ Unlike the adversarial litigation process, mediation assists in establishing a helpful dialogue, particularly in the situations of high-stakes data breach when relationships between businesses and the reputation are essential.² The fact that mediation is not binding means that the parties are in control of the result, but voluntary collaboration and good-faith participation is paramount to its effectiveness.

1.2. Arbitration

The confidential judicial process is called arbitration, the decision of which, made by one or more arbiters, appointed due to their professional competence in the field of cybersecurity law and technology, is

¹ Dada SO and Jimoh FB, "Forensic Accounting and Financial Crimes in Nigerian Public Sector" *Journal of Accounting and Taxation* 12, no. 4. (October 31, 2020): 118. <<https://doi.org/10.5897/jat2020.0417>>

² Akintayo, Obafemi D, Chinazo Nneka Ifeanyi, and None Okeoma Onunka. "Resolving Cybersecurity Disputes and Protecting Digital Infrastructure With ADR." *Computer Science & IT Research Journal* 5, no. 10 (October 24, 2024): 2437. <<https://doi.org/10.51594/csitrj.v5i10.1674>>

binding and does not involve the procedure of going to court.³ The approach is highly utilized in the process of data breach litigations because of its enforceability, procedural efficiencies, and the ability of the arbitrators to have technical expertise.⁴ The binding nature of arbitration however limits the chances of appeal and this fact can be a deterrence to some parties to employ this procedure.

1.3. Negotiation

Negotiation can be defined as a direct communication between the conflicting parties in an attempt to resolve the conflict without involving third parties.⁵ As much as negotiation is the most adaptive and affordable method, it may only succeed when there is a desire to cooperate with each other and the power differences are not significant. Negotiation may be the most appropriate when faced with data breach and the most significant considerations in the conflict are confidentiality and speed.

1.4. Expert Determination

Expert determination is a procedure that involves appointing a qualified expert to examine the issue and arrive at a binding decision in technically complex situations.⁶ This practice is especially topical in such cases when the conflict with cybersecurity is connected with a complex study of the forensic evidence or the adherence to the regulatory norms. However, the binding nature of expert determination may be inappropriate in instances in which the parties are not interested in the final decision but rather a further cooperation.

1.5. Conciliation

Similar to mediation, conciliation relies on the third party that is neutral to assist in solving the problem, the conciliator can however be more advisory in nature to generate solutions.⁷ It is not as formal as arbitration but has a structured guidance and can therefore be applied in situations where parties require moderate intervention to clear impasses.

1.6. Early Neutral Evaluation (ENE)

ENE is a preliminary assessment process through which an independent reviewer investigates the legitimacy of a cybersecurity breach claim to determine the type of settlements that could be done.⁸ Even though ENE can help in resolving the disputes by clarifying central issues, it is not effective unless there are powerful enforcement programs that will make it effective in case of failure to comply with evaluative recommendations.

³ Veena T. N. "Misappropriation of Trade Secrets Under the Indian Legal Framework: An Analytical Study." *Christ University Law Journal* 12, no. 1 (July 25, 2023): 180. ><https://doi.org/10.12728/culj.22.4>>

⁴ Akintayo, Ifeanyi and Onunka (n 2), 1440.

⁵ U, Dhivya. "Pivotal Significance of Alternative Dispute Resolution Within the Realm of Financial Institutions." *Journal of Law and Legal Research Development* 1, no: 2 (May 30, 2024): 3. <<https://doi.org/10.69662/jllrd.v1i2.8>>

⁶ Dada and Jimoh, "Forensic Accounting", 120.

⁷ Veena, "Misappropriation", 183.

⁸ Rustambekov, Islambek. "Features of the Settlement of International Cyber Disputes Through ADR in the Context of the Legislation of the BRICS Countries." *Ticaret Ve Fikri Mülkiyet Hukuku Dergisi* 10, no. 1 (June 30, 2024): 152. <<https://doi.org/10.55027/tfm.1379346>>

1.7. Online Dispute Resolution

ODR has come up as a particular platform to address issues in the digital world such as data breaches unlike other disputes and conflicts that have been on the rise in the digital world.⁹ ODR is a technology enabled means to make remote negotiation, mediation or arbitration scalable and accessible. Nevertheless, some of the aspects that require improvement still exist, including data security and jurisdictional uniformity.

1.8. Ombudsmen Services

Ombudsmen are the free authorities who investigate the complaints and discuss the resolutions which are often employed in the institutional or governmental environment to fight with the maladministration and in this context cyber wars particularly.¹⁰ They are not normally binding and they are useful when resolving disputes where there are systematic problems or repeated complaints.

2. Mediation in Data Breach Disputes

It has also been established that mediation is a potent instrument in resolving the data breach dispute since it is a collaborative way of resolving a dispute where the parties in dispute can iron out their differences with the assistance of neutral mediators who help them to achieve a solution that will satisfy both sides.¹¹ Unlike adversarial litigation, mediation relies on a third party that is deemed to be neutral and helps parties to a dispute obtain negotiated settlements without having to make binding judgments, which results in the creation of voluntary and consensual outcomes.¹² The strategy is specifically helpful in the case of data breaches because it ensures positive communication, enhanced understanding, and the development of tailor-made solutions that may be applied during the consideration of the interests of the parties involved.¹³ Mediation is also in line with the need for subtle solutions to digital conflicts that are complicated since it is more about collaboration than it is about conflict.

2.1. Advantages of Mediation in Data-Related Conflicts

The conflict based on the personal data breach should be resolved through mediation as a suitable means due to the inherent flexibility that has several crucial benefits, including affordability, confidentiality, and flexibility of the process, and time-saving.¹⁴ These are the benefits that are necessary in online litigation where the conventional litigation is either too costly or time-consuming. Most of the data-related conflicts can be solved with the help of mediation that implies the integration of legal solutions, such as data deletion or compensation along with negotiated settlements.¹⁵ Furthermore, cross-border data disputes may also be governed by international systems, e.g., the Singapore Convention on Mediation, that allows resolving any

⁹ Rustambekov, "Features of the Settlement", 154.

¹⁰ Rustambekov, "Features of the Settlement", 158.

¹¹ Dewi, Sinta, Robert Walters, Leon Trakman, and Bruno Zeller. "The Role of International Mediation in Data Protection and Privacy Law - Can It Be Effective?" *Australian Dispute Resolution Journal* 30, no: 61 (January 1, 2019): 20. <<https://doi.org/10.2139/ssrn.3462113>>

¹² Rasji Lewiandy and Samantha Elizabeth Fitzgerald, "The Role of Mediation as A Form of Amicable Settlement Prior to Arbitral Proceedings under Bani Arbitration Center Rules and Procedures," *International Journal of Application on Social Science and Humanities* 1, no. 1 (20 February 2023): 70. <<https://doi.org/10.24912/ijassh.v1i1.25688>>

¹³ Akintayo, Ifeanyi and Onunka, "Resolving Cybersecurity", 2441.

¹⁴ Subhashini S, "The Use Of ADR in Resolving Disputes Related to Social Media and Online Platforms," *Russian Law Journal* 11, no. 3 (7 Nisan 2023): 2463. <<https://doi.org/10.52783/rj.v11i3.2139>>

¹⁵ Steinly Suwanto Putra and Nynda Fatmawati Octarina, "Legal Protection for Neighborhood Association Administrations in the Implementation of Personal Data Collection Duties," *International Journal of Humanities Education and Social Sciences (IJHESS)* 3, no. 5 (11 April 2024): 140. <<https://doi.org/10.55227/ijhess.v3i5.766>>

jurisdictional complexities in a systematic manner, which is an alternative to protracted litigation.¹⁶ These frameworks promote the enforceability of mediated arrangements in a cross-border setting, which is one of the major challenges in international data breaches.

2.2. Mediation in High-Stakes Cybersecurity Contexts

Mediation is a tactical conflict management instrument in high stakes cybersecurity scenarios where the most considerable activity is the maintenance of business relations and reputation safeguarding. With the aid of mediation, companies that have fallen victims of data breaches can resolve conflicts without ruining relationships and winning the trust of their customers.¹⁷ In addition, mediation enhances access to justice particularly in such jurisdictions where legal expenses may be prohibitive to the affected individual or smaller organizations to seek recourse to formal legal proceedings.¹⁸ Mediation also assists in overcoming the immediate effects of data breaches besides assisting in fostering trust and regulatory compliance among the stakeholders in the long term by offering a friendlier and more accessible dispute resolution process. As a result, its role in dispute settlement in cybersecurity is likely to grow since the issues of data protection are becoming much more complicated.

3. Arbitration as an ADR Mechanism in Data Breach Conflicts

The arbitration method of resolving the dispute on data breach is the most notable ADR process that renders binding solutions through the help of independent third-party arbitrators with knowledge of cybersecurity law and technology. Unlike mediation, which encourages negotiations without passing a binding decision, arbitration is a final and binding decision, and therefore it will accelerate the process of compliance with cybersecurity rules.¹⁹ The fact that the arbitrators are selected by the parties involved in the dispute is one of the strongest aspects of the arbitration procedure because the parties have the guarantee that the experts selected possess the technical and legal skills to solve complex data breach cases.

The level of acceptance of the arbitration in the resolution of disputes over the personal data has reached a considerable degree, particularly, in the cross-border context under the regulations such as the European Union General Data Protection Regulation.²⁰ Arbitration has been formally recognized as a legitimate means of resolving data protection disputes in many jurisdictions and the law is enacted to permit arbitration as a choice, besides litigation and other types of ADR. This legal justification can apply even in international electronic transactions wherein the involved parties may still have the option of choosing arbitration courts to adjudicate on the arising disputes as a result of cross-border transfer of information.²¹ This is what renders arbitration more suitable to multinational companies and organizations which engage in cross-nation transfer of data.

¹⁶ Dewi and others, "The Role of International Mediation", 22.

¹⁷ Akintayo, Ifeanyi and Onunka, , "Resolving Cybersecurity", 2445.

¹⁸ Beduschi A., "Rethinking Digital Identity for post-COVID-19 Societies: Data Privacy and Human Rights Considerations," *Data & Policy*, no. 3 (January 1, 2021): e15-3. <<https://doi.org/10.1017/dap.2021.15>>

¹⁹ Akintayo, Ifeanyi and Onunka, , "Resolving Cybersecurity", 2447.

²⁰ Trakman L., Walters R. and Zeller B., "Is International Arbitration Prudent When Dealing With Personal Data Challenges?," *SSRN Electronic Journal* (January 1 2019): 5 <<https://doi.org/10.2139/ssrn.3503176>>.

²¹ Mentari N., Nugraheni N. and Annas M., "Legal Protection of HARA Platform Users on the Service of Electronic Data Interchange" *Jurnal Hukum Novelty* 14, no. 1 (2023): 51. <<http://dx.doi.org/10.26555/novelty.v14i1.a25547>>

Some of the distinct benefits of arbitration when used in the context of data breach claims include the confidentiality of the court proceedings, shorter resolution timelines, and flexibility of the proceedings in comparison to common litigation. Considering that data breach cases are sensitive matters, certain processes have been developed using the modern arbitration systems in order to safeguard sensitive information. To illustrate, the Electronic Security Protocol in Commercial Arbitration establishes all the rules of ensuring sensitive data during the arbitration process, such as confidentiality agreements, access control, and prepared incident response strategies.²²

The arbitration procedure may be particularly helpful in the case of interstate conflict that may arise in cyberspace, i.e., conflict over cyberattacks, international data transfer, and limitations of digital rights.²³ Its formal and flexible nature leaves the likelihood of utilizing it as an instrument that can be applied to solve complicated international data breach incidents without destroying business relationships. Sustainable conflict resolution in the digital sphere can be achieved through arbitration, since the process of its resolution will be more efficient and friendly than that of litigation.

4. Advantages of ADR in Data Breach Disputes

ADR mechanisms have immense benefits in comparison to litigation in settling disputes that arise in cases of data breaches, and hence they cover serious issues that are of paramount importance, like cost, efficiency, confidentiality, and accessibility. These are the advantages that render ADR especially applicable to the cases of online disputes, such as cyberbullying, defamation in the online sphere, and leaking sensitive information.²⁴

Some of the most outstanding advantages of ADR include that it is relatively cheaper and more expedient as compared to the judicial proceedings. Traditional litigation procedure may be lengthy and expensive in terms of legal services provided, but ADR procedures (i.e., mediation and arbitration) can be less time- and resource-consuming.²⁵ This is critical in the case of data breaches since it can aggravate the harm caused to the affected individuals and organizations when delayed.²⁶ ADR allows the parties to minimize the reputational loss and money loss quicker without going through lengthy litigation.

Unlike the court trials, ADR proceedings are confidential and therefore sensitive information does not make its way into the general sphere. This confidentiality is particularly helpful when dealing with data breach, whereby publicity can further worsen the reputation of an organization and affect the faith of stakeholders. Moreover, the closed-door resolutions enable the maintenance of business relations, as the parties to an agreement are not afraid of unfavourable publicity.²⁷ As the data protection area becomes increasingly regulated, the privacy-preserving nature of ADR will enable the companies to comply with the minimum possible reputational harm.

²² Asmaa Saad Hussien and Hani Mohamed Mounes, "Cybersecurity in International Commercial Arbitration (Legal Vision)," *International Journal of Advanced and Applied Sciences* 11, no. 2 (February 1, 2024): 219–229. <<https://doi.org/10.21833/ijaas.2024.02.023>>

²³ Joanna Kulesza, "Peaceful Settlement of Interstate Online Disputes," *Laws* 11, no. 3 (June 8, 2022): 49.

²⁴ Subhashini, "The use of Adr", 2465.

²⁵ Veena, "Missappropraiton", 185.

²⁶ Saputro, M Susilo Agung, Nanda Puspitasari Wardoyo, Nurani Sofiyana, Shahnata Putri Dwi Ramadhani, and Aris Prio Agus Santoso. "Consumer Protection in Online Shopping." *Mutiara Multidisciplinary Scientific Journal* 2, no. 4 (April 29, 2024): 222–228. <<https://doi.org/10.57185/mutiara.v2i4.174>>

²⁷ Akintayo, Ifeanyi and Onunka, , "Resolving Cybersecurity", 2446.

ADR offers the atmosphere of cooperation, in which the sides are encouraged to negotiate and find a solution that would fit both.²⁸ Such an approach is especially applicable in cases of cybersecurity conflicts when the long-term business relationship is typically just as significant as resolving the specified conflict. ADR is adaptable and capable of offering tailored solutions that would take into account the technical and legal complexities of data breaches, cross-border disputes included.²⁹ In addition, the arbitration enables the appointment of expert neutrals that possess knowledge on cybersecurity to settle the disputes, and this is binding and informed.³⁰

ADR can be described as a democratization of conflict resolution because it provides easy access to legal resolutions to non-elite citizens or smaller entities that may not be able to afford a conventional lawsuit.³¹ In the instance of data breach, where the victim consumers are up against well-funded corporations, ADR provides a level playing ground, and thus equal access to justice. This is especially important in those jurisdictions where litigation is expensive, and in such cases ADR is an effective alternative to resolving digital disputes.

The data flows are global and the dispute resolution mechanisms should be in a position to settle transnational conflicts. This cross-border flexibility of ADR might be relevant to cross-border data breach scenarios as well as the structures through which such multi-jurisdictional collaboration is facilitated (including the Mutual Legal Assistance Treaties (MLATs)).³² This kind of global accessibility allows parties to reach enforceable solutions even despite the existence of disparities between the legal systems in question and increases the adherence to cybersecurity standards worldwide.³³

5. Challenges and Limitations of ADR in Data Breach Cases

In as much as there are some benefits that have been admitted to the ADR methods, its application in the data breach cases brings some serious challenges that limit its effectiveness. The initial one is the size of the claimants involved in the typical case. Data breaches may concern thousands or even millions of individuals affected and the application of the standard ADR processes may be problematic, as the model of dispute resolution in question is normally expected to manage a small number of parties involved in a dispute.³⁴ Calculating the logistical and operational challenge of large claims is one of the questions that cast a shadow of doubt on the viability of ADR in such environment.

Another challenge is that the implementing regulations and legal precedent are not apparent, so they can be applied to the situations of data breaches. Unlike the typical business dispute where the ADR systems have a certain structure, the breach of data cases are on a very new legal basis. Claimants and respondents are in a dilemma since there are no standardized practices to adhere to or guidelines in the court on how ADR is

²⁸ Dhivya, "Pivotal Significance", 5.

²⁹ Aussielia Amzulian, "The Future of Arbitration for Personal Data Disputes in Indonesia: Weighing the Benefits and Challenges," *Media Iuris* 8, no. 2 (June 30, 2025): 215. <<https://doi.org/10.20473/mi.v8i2.63060>>

³⁰ Akintayo, Ifeanyi and Onunka, "Resolving Cybersecurity", 2446.

³¹ Beduschi, "Rethinking Digital Identity", e15-5.

³² Jaskaran Singh Saini et al., "Cloud Computing: Legal Issues and Provision," *Security and Communication Networks* (August 1 2022): 2 <<https://doi.org/10.1155/2022/2288961>>

³³ Amzulian, "The Future of Arbitration", 217.

³⁴ Amzulian, "The Future of Arbitration", 218.

supposed to be done.³⁵ This regulatory gap renders it hard to build up consistent and predictable methods of settling such disputes.

Financial and procedural burdens are also a major challenge especially to individual data subjects who wish to seek redress. Although ADR might be an economical option to organizations in comparison to litigation, the costs of formal dispute resolution procedures can still be prohibitive to individuals, in particular when the value of damages is not very high.³⁶ This imbalance in the economy may be a deterrence to taking part and aggravation of equitable settlement of claims.

The question of obtaining valid consent of data subjects is one of the inherent issues of international arbitration regarding the cases of data breaches. Another legal and ethical dilemma is that to overcome the conflict of misusing the personal information of the affected people, it is necessary to carry out further processing of their personal information.³⁷ This requirement complicates the process and may exclude the claimants who do not desire or can refuse to provide additional use of data.

The empirical studies indicate that arbitration is untested practice in disputes involving privacy. Studies indicate that there is an extreme gap between the privacy rights of adjudicated cases, those that have been adjudicated through arbitration despite the prevalence of arbitration clauses in consumer contracts.³⁸ This precedential gap can be termed as the misconstruing of procedural fairness, predictability of outcome and the adaptability of ADRs to the demands of data breach conflicts.

ADR is also ineffective in data breach due to security problems. Organizations may decide to settle unfairly in arbitration in an effort to hide trade secrets and sensitive information.³⁹ As much as the arbitration organizations have devised special protocols to enhance the security of the information, like technical protection and securing the participants, they introduce more complexity and cost.⁴⁰ A very critical constraint is also enforcement particularly in non-binding ADR mechanisms. As an example, early neutral evaluation, as beneficial as it can be in diagnosing breach, requires effective enforcement systems to ensure the compliance with it that may not be present in voluntary systems.⁴¹

6. Practical Implementation of ADR Mechanisms for Data Breach Disputes

The increasing rate of data breaches has seen several jurisdictions in progress with legal frameworks that recognize and give preference to ADR mechanisms clearly. These structures are supposed to provide efficient, flexible and secretive methods of dispute resolution and relieve the burden of the traditional courts. Indonesia is a good example that enacted the Personal Data Protection Law (PDP Law) which has both preventive and repressive data protection provisions. Interestingly, the law also gives the parties an alternative on how to settle disputes by arbitration, therefore, offering legal certainty and an incentive to businesses to employ more flexible methods of settling disputes. The strategy highlights the increased

³⁵ Amzulian, "The Future of Arbitration", 220.

³⁶ Amzulian, "The Future of Arbitration", 220.

³⁷ Trakman and others, "Is International Arbitration Prudent", 7.

³⁸ Rustambekov, "Features of the Settlement", 155.

³⁹ Hussien, "Cybersecurity", 220.

⁴⁰ Hussien, "Cybersecurity", 225.

⁴¹ Rustambekov, "Features of the Settlement" 157.

awareness of the appropriateness of ADR to data-related claims as it is more efficient, confidential and transnational.⁴²

6.1. Legal Frameworks and Institutional Support

The effective introduction of ADR in the framework of data breach conflicts could not be narrowed down to the legislative acceptance and would in fact necessitate the existence of institutional frameworks which are specialized. It has been demonstrated that governments should establish sector-specific arbitration boards which are intended to address the peculiarities of the data disputes including mass claims, regulatory complexity, the necessity of technical knowledge.⁴³ The process of solving problems can be simplified, rendered less expensive, and more accessible to the parties by specialized bodies. In addition, it is imperative that effective implementing rules and precedents should be established to ensure that ADR frameworks are functional with the predictability and efficiency they must have. Without them, the finest-designed legal rules may not provide any benefits that are intended as compared to traditional litigation.

6.2. Tiered and Graduated Dispute Resolution Processes

According to the best practices of ADR implementation, they should apply the tier system under which the dispute is settled one by one- online negotiation, mediation, and arbitration in which the unsolved dispute is then left in court.⁴⁴ Such a gradual model will ensure that less confrontational, less complex avenues are exhausted first before arbitration is resorted to in more stubborn cases. Legal frameworks of various jurisdictions have now clearly authorized the ADR mechanisms by enabling parties to settle disputes through the means of arbitration or other alternative institutions by the use of the pertinent laws. In the case of the cross-border data breaches, the parties would also be allowed to appoint arbitration tribunals or dispute resolution organizations that are specialized in international electronic transactions.⁴⁵

6.3. The Role of Online Dispute Resolution

The data breaches on the internet have increased the speed of the ODR systems being adopted to integrate negotiation, mediation, and arbitration online.⁴⁶ The new developments offer AI-based conflict resolution systems which can process forensics evidence and peer-to-peer conflict resolution between the consumers and the service providers.⁴⁷ These innovations eliminate some of the key issues in the data breach litigations, such as speed of resolution and technical expertise. Availability of ODR is also enhanced by the new generation of ODR sites which offer mediation, arbitration and binding opinions through fair, expedited and cost-effective procedures. It is particularly important to individuals and other smaller parties who might not have the money to pursue a traditional litigation.

⁴² Amzulian, "The Future of Arbitration", 222.

⁴³ Amzulian, "The Future of Arbitration", 223.

⁴⁴ Sulistianingsih, Dewi, Alviona Anggita Rante Lembang, Yuli Prasetyo Adhi, and Muchammad Shidqon Prabowo. "Online Dispute Resolution: Does the System Actually Enhance the Mediation Framework?" *Cogent Social Sciences* 9, no. 1 (May 4, 2023): 3. <<https://doi.org/10.1080/23311886.2023.2206348>>

⁴⁵ Mentari and others, "Legal Protection", 55.

⁴⁶ Laurie Butgereit, "Data Considerations for a Smart Fourth Party in an Online Dispute Resolution System," içinde *International Conference on Intelligent Engineering Systems* (July 26, 2023), 73–76 <<https://doi.org/10.1109/ines59282.2023.10297758>>.

⁴⁷ Abdullah Mujawib Alashjaee, "Toward a Conflict Resolution Protocol for Cloud Forensics Investigation," *IEEE Access* 12 (1 January 2024): 72013–22. <<https://doi.org/10.1109/access.2024.3402623>>.

Conclusion

The review of the Alternative Dispute Resolution mechanisms applied to the dispute of the data breaches highlights the increasing importance of the ADR mechanisms as possible alternatives to the traditional litigation. ADR approaches (such as mediation, arbitration, negotiation, expert determination and online dispute resolution) have unique benefits to handle the intricacies of data-related disputes. The advantages of the mechanisms are cost-effective, time-saving, and confidentiality, especially when it comes to the cases of high-stakes cybersecurity disputes, where reputation and sensitive information are involved. In addition, ADR is more flexible and collaborative, and it also offers differentiated solutions that litigation cannot readily offer, which improves access to justice among the affected parties. As much as this may be the advantages, there are grave concerns involved in the use of ADR in cases of data breaches. The lack of regulation and precedents especially in transnational cases may impede uniform application and the issue of access to costs and ethics of consent will have to be examined further. Moreover, the safety of ADR procedures and the validity of outcomes remain to be a pressing issue, especially in the case of interstate cyber conflicts when the problem of jurisdiction is involved. These deficiencies should be addressed with effective legislation, institutional assistance and incorporation of multi-level dispute resolution systems that can be adapted to the nature of the new cyber threats. The focus of the research on the possibility of utilizing the emerging technologies such as blockchain and artificial intelligence to make the ODR platforms more efficient and how the standard procedures could be developed that would be implemented to use ADR in case of a data breach should be the focus of the future studies. Because holes that exist are filled, and interdisciplinary cooperation between legal professionals, professionals in the technical disciplines, and policy professionals are promoted, ADR would become a foundation of effective and fair dispute resolution in the digital age. Lastly, there will be a need to enhance ADR mechanisms further as the effort is made to strike a balance between the conflicting interests of privacy, security and justice in an increasingly globalized world.

Değerlendirme / Review

This article was peer-reviewed by at least two independent reviewers and screened for plagiarism, it complies with research and publication ethics, licensed under CC BY-NC 4.0.

Beyanlar / Declarations

No ethics committee approval was required. The author is solely responsible for all aspects of the study and manuscript. No funding was received, and there are no conflicts of interest to declare. AI tools were used only for language editing and improving the fluency and readability of the manuscript; the author takes full responsibility for the final content.

Bibliography

- Akintayo, Obafemi D, Chinazo Nneka Ifeanyi, and None Okeoma Onunka. "Resolving Cybersecurity Disputes and Protecting Digital Infrastructure With ADR." *Computer Science & IT Research Journal* 5, no. 10 (October 24, 2024): 2437–57. <https://doi.org/10.51594/csitrij.v5i10.1674>.
- Alashjaee, Abdullah Mujawib. "Toward a Conflict Resolution Protocol for Cloud Forensics Investigation." *IEEE Access* 12 (January 1, 2024): 72013–22. <https://doi.org/10.1109/access.2024.3402623>.
- Amzulian, Aussielia. "The Future of Arbitration for Personal Data Disputes in Indonesia: Weighing the Benefits and Challenges." *Media Iuris* 8, no. 2 (June 30, 2025): 215–38. <https://doi.org/10.20473/mi.v8i2.63060>.
- Beduschi, Ana. "Rethinking Digital Identity for post-COVID-19 Societies: Data Privacy and Human Rights Considerations." *Data & Policy*, no. 3 (January 1, 2021): e15. <https://doi.org/10.1017/dap.2021.15>.
- Butgereit, Laurie. "Data Considerations for a Smart Fourth Party in an Online Dispute Resolution System." *International Conference on Intelligent Engineering Systems*, (July 26, 2023): 73–76. <https://doi.org/10.1109/ines59282.2023.10297758>.
- Dada, Samuel O., and Fatai B. Jimoh. "Forensic Accounting and Financial Crimes in Nigerian Public Sector." *Journal of Accounting and Taxation* 12, no. 4 (October 31, 2020): 118–25. <https://doi.org/10.5897/jat2020.0417>.
- Dewi, Sinta, Robert Walters, Leon Trakman, and Bruno Zeller. "The Role of International Mediation in Data Protection and Privacy Law - Can It Be Effective?" *Australian Dispute Resolution Journal* 30, no: 61 (January 1, 2019): 19-77. <https://doi.org/10.2139/ssrn.3462113>.
- Hussien, Asmaa Saad, and Hani Mohamed Mounes. "Cybersecurity in International Commercial Arbitration (Legal Vision)." *International Journal of Advanced and Applied Sciences* 11, no. 2 (February 1, 2024): 219–29. <https://doi.org/10.21833/ijaas.2024.02.023>.
- Kulesza, Joanna. "Peaceful Settlement of Interstate Online Disputes." *Laws* 11, no. 3 (June 8, 2022): 49-62. <https://doi.org/10.3390/laws11030049>.
- Lewiandy, None, None Rasji, and Samantha Elizabeth Fitzgerald. "The Role of Mediation as A Form of Amicable Settlement Prior to Arbitral Proceedings under Bani Arbitration Center Rules and Procedures." *International Journal of Application on Social Science and Humanities* 1, no. 1 (February 20, 2023): 67–75. <https://doi.org/10.24912/ijassh.v1i1.25688>.
- Mentari, Nikmah, Ninis Nugraheni, and Muhammad Annas. "Legal Protection of HARA Platform Users on the Service of Electronic Data Interchange." *Jurnal Hukum Novelty* 14, no. 1 (April 30, 2023): 51-68. <https://doi.org/10.26555/novelty.v14i1.a25547>.
- Putra, Steinly Suwanto, and Nynda Fatmawati Octarina. "Legal Protection for Neighborhood Association Administrations in the Implementation of Personal Data Collection Duties." *International Journal of Humanities Education and Social Sciences (IJHESS)* 3, no. 5 (April 11, 2024): 2732-8. <https://doi.org/10.55227/ijhess.v3i5.766>.

- Rasji Lewiandy and Samantha Elizabeth Fitzgerald, "The Role of Mediation as A Form of Amicable Settlement Prior to Arbitral Proceedings under Bani Arbitration Center Rules and Procedures," *International Journal of Application on Social Science and Humanities* 1, no. 1 (20 February 2023): 67–75. <<https://doi.org/10.24912/ijassh.v1i1.25688>>
- Rustambekov, Islambek. "Features of the Settlement of International Cyber Disputes Through ADR in the Context of the Legislation of the BRICS Countries." *Ticaret ve Fikri Mülkiyet Hukuku Dergisi* 10, no. 1 (June 30, 2024): 149–66. <https://doi.org/10.55027/tfm.1379346>.
- Saini, Jaskaran Singh, Dinesh Kumar Saini, Punit Gupta, Chhattar Singh Lamba, and G. Madhusudhana Rao. "Cloud Computing: Legal Issues and Provision." *Security and Communication Networks* (August 1, 2022): 1–13. <https://doi.org/10.1155/2022/2288961>.
- Saputro, M Susilo Agung, Nanda Puspitasari Wardoyo, Nurani Sofiyana, Shahnata Putri Dwi Ramadhani, and Aris Prio Agus Santoso. "Consumer Protection in Online Shopping." *Mutiara Multidisciplinary Scientific Journal* 2, no. 4 (April 29, 2024): 222–228. <https://doi.org/10.57185/mutiara.v2i4.174>.
- Steinly Suwanto Putra and Nynda Fatmawati Octarina, "Legal Protection for Neighborhood Association Administrations in the Implementation of Personal Data Collection Duties," *International Journal of Humanities Education and Social Sciences (IJHESS)* 3, no. 5 (11 April 2024): 137–158. <https://doi.org/10.55227/ijhess.v3i5.766>.
- Subhashini, None S. "The Use of ADR in Resolving Disputes Related to Social Media and Online Platforms." *Russian Law Journal* 11, no. 3 (April 7, 2023): 2462–2473. <https://doi.org/10.52783/rlj.v11i3.2139>.
- Sulistianingsih, Dewi, Alviona Anggita Rante Lembang, Yuli Prasetyo Adhi, and Muchammad Shidqon Prabowo. "Online Dispute Resolution: Does the System Actually Enhance the Mediation Framework?" *Cogent Social Sciences* 9, no. 1 (May 4, 2023): 1–14. <https://doi.org/10.1080/23311886.2023.2206348>.
- Trakman, Leon, Robert Walters, and Bruno Zeller. "Is International Arbitration Prudent When Dealing With Personal Data Challenges?" *SSRN Electronic Journal*, (January 1, 2019): 1–24. <https://doi.org/10.2139/ssrn.3503176>.
- U, Dhivya. "Pivotal Significance of Alternative Dispute Resolution Within the Realm of Financial Institutions." *Journal of Law and Legal Research Development* 1, no. 2 (May 30, 2024): 1–12. <https://doi.org/10.69662/jllrd.v1i2.8>.
- Veena, T. N. "Misappropriation of Trade Secrets Under the Indian Legal Framework: An Analytical Study." *Christ University Law Journal* 12, no. 1 (July 25, 2023): 166–200. <https://doi.org/10.12728/culj.22.4>.