AMERICAN JOURNALS
Open Access, Peer Reviewed Journals

American Journal of Technology and Applied Sciences
ISSN (E): 2832-1766| Volume 17, | October., 2023

LIABILITY FOR CYBERATTACKS IN ONLINE DISPUTE RESOLUTION

PhD. Якубова Мадинабону Абдумаликовна
Тошкент давлат юридик университети кибер хукук кафедраси

A B S T R A C T

This article discusses the issue of liability for cyberattacks in online dispute resolution (ODR). As ODR grows in popularity as a means of effective and affordable dispute resolution, questions arise regarding liability when the ODR platform itself is at risk from a cyberattack. Based on an analysis of relevant case law and legislation, the paper argues that the current legal framework is inadequate to address this issue of problem. A review of technological solutions points to blockchain as a promising tool for improving security and ensuring a better distribution of responsibility after an attack. However, technology alone is not enough. The document proposes legislative and policy changes to clearly delineate the responsibilities of ODR platform providers and users to prevent attacks. and a compensation fund model to support reparations in the event of attacks. By clarifying liability and providing compensation, these measures can contribute to the sustainable development of ODR as a fair and reliable means of dispute resolution.

K E Y W O R D S

Online dispute resolution, cybersecurity, cyberattacks, liability, liability, compensation fund.

Introduction

Online dispute resolution (ODR) offers convenient and cost-effective means of resolving conflicts through technological communication, negotiation, and decision-making (Katsh & Rule, 2015). Through ODR platforms, parties can easily access mediation, arbitration, ombudsman services, and other dispute resolution options entirely online. The COVID-19 pandemic has accelerated the adoption of ODR in various sectors, including e-commerce, healthcare, banking, and courts (Levin, 2020). However, as the scope and reach of ODR expands, there are concerns about cyberattacks that could compromise ODR platforms and processes (Cui, 2021). Who is responsible if cyberattacks or other technological failures prevent access to ODR services or corrupt dispute resolution procedures? This article examines the issue of accountability for cyberattacks in SOE through doctrinal and legal analysis, a review of technological solutions, and proposals for legislative and policy reforms.

Methodology: This article uses a qualitative doctrinal methodology, analyses relevant case law, legislation, and academic literature to examine how the existing legal framework governs liability for

cyberattacks affecting ODR. Cases involving online security breaches in various industries are reviewed in order to clarify the current legal situation. Laws and regulations governing ODR providers and participants are reviewed to determine whether they adequately delineate duties and responsibilities in relation to cyberattacks. The article complements this doctrinal legal analysis by looking at technological tools that have the potential to enhance ODR security, as well as legislative and policy proposals put forward by legal scholars that seek to clarify liability.

Theoretical Outcomes: Doctrinal analysis shows that there is currently no clear framework for determining responsibility for cyberattacks on ODR platforms and procedures. The general principles of tort law related to negligence and product liability can in some cases lead to ODR providers being at fault for lack of safety (Moringiello & Reynolds, 2018). However, the results are uncertain given the novelty of ODR. Contract law also does not provide predictability, as the terms of service of ODR service providers often exclude or limit liability. Laws such as the U.S. Electronic Signatures in Global and National Commerce Act regulate the validity of electronic transactions but do not impose responsibility for technological failures. Cases of cyberattacks on e-commerce companies show conflicting standards as to whether technology providers or end-users are responsible for security breaches (Boulware, 2022). Thus, doctrinal analysis shows that the existing legal framework is inadequate to address issues of liability for cyberattacks in the context of ODR.

The Technology Review identifies new solutions that have the potential to mitigate ODR cybersecurity risks. Blockchain-based ODR platforms use decentralized networks to prevent centralized points of failure (O'Brennan, 2021). Cryptographic techniques such as digital signatures, encryption, and access control can help protect ODR data and communications (Schmitz, 2019). Artificial intelligence can monitor ODR systems for suspicious activity indicative of attacks (Cui, 2021). While technology can significantly improve ODR security, gaps and human error remain. Purely technological solutions are also limited in their ability to determine responsibility for successful attacks. This implies the need for legal and policy measures to complement advances in cybersecurity.

Actionable Outcomes: To address accountability gaps, legislators at the national and international level should enact targeted laws and regulations to ensure ODR safety. They should clearly define the responsibilities of ODR providers to implement reasonable cybersecurity measures and consistently monitor systems for risks (Katsh & Rule, 2015). Laws should also prescribe terms of service for the ODR platform, requiring users to maintain secure access credentials and promptly report suspicious activity. Legislation can build on standards such as ISO/IEC 27701 to enable ODR providers to apply best practices for cyber risk management. It is important to note that laws should establish criteria for establishing liability in the event of disputes arising over attacks on platforms. Clear provisions are needed to impose liability between ODR providers and users on the basis of negligence,

In addition to laws, policy measures should create compensation funds for ODR cyberattacks. These no-fault pools could support indemnification to parties who have suffered losses in the event of a platform security breach (Schmitz, 2019). Compensation funds can recover damages without lengthy liability court proceedings. The fund's capital can be generated through fees charged to ODR providers and mandatory contributions corresponding to the platform's profits. For the ODR industry to be trusted at all times, prompt compensation must be available in the event of cyberattacks, regardless of legal liability.

In order for ODR vendors and users to prevent attacks and recover losses, a combination of technological, legislative, and policy changes are needed. These measures will contribute to the

sustainable growth of ODR by transparently defining responsibilities between stakeholders and response protocols in the event of a cybersecurity failure. ODR's enormous promise for ensuring accessible and effective justice depends on ensuring that it is resilient to emerging cyber threats through proactively strengthening accountability mechanisms.

Conclusion: As online dispute resolution spreads across the globe, cyberattacks pose a serious threat to the procedural integrity and interests of participants. The existing legal framework does not provide adequate clarity on liability for technological failures that jeopardize SOE. While promising cybersecurity technologies such as blockchain can partially mitigate risks, technology alone cannot determine liability or provide redress in the event of attacks. This document argues that targeted legislation, regulations and policies are needed to define responsibilities among OE stakeholders, allocate responsibility for incidents, and establish compensation funds. Clarifying the scope of accountability is necessary to ensure accountability, redress, and maintain the credibility of ODR as a fair means of dispute resolution appropriate to the digital age.

References:

1. Bulvar, J.T. (2022). Accountability for e-commerce cyberattacks: Putting the blame where it belongs. Yale Journal of Law and Technology, 14(1), 273–305.
2. Cui, L. (2021). Secure online dispute resolution (ODR) with artificial intelligence. Review of the Law of the Asia-Pacific Region, 28(2), 187–199.
3. Katsch, E., & Ruhl, K. (2015). What We Know and Need to Know About Online Dispute Resolution. South Carolina Law Review, 67(2), 329–336.
4. Levin, V. (2020). Online Dispute Resolution: The Impact of COVID-19. Seton Hall Law Review, 51(4), 1019–1031.
5. Moringiello J. and Reynolds, W. (2018). From LORD Coke to Online Privacy: The Past, Present, and Future of Electronic Contract Law. Review of Rutgers Law, 71(1), 421–446.
6. O'Brennan, J. (2021). Online Dispute Resolution Using Blockchain: A New Form of Justice for Commerce and Consumers. Notre Dame Journal of Law, Ethics, and Public Policy, 35(1), 101–124.
7. Schmitz, A.J. (2019). Ensuring online dispute resolution. Florida Law Review, 71(6), 1217–1256.