doi:10.1017/aju.2024.4

SYMPOSIUM ON DIGITAL EVIDENCE

DIGITAL EVIDENCE IN DISPUTES INVOLVING STATES

Daniel Brantes Ferreira and Elizaveta A. Gromova***

The use of digital evidence increases concurrently with increased digitalization of the larger world and of justice processes. This essay aims to address the use of digital evidence in interstate disputes and other disputes involving states. It focuses on the case law of two international arbitral bodies—the Permanent Court of Arbitration (PCA) and the International Centre for Settlement of Investment Disputes (ICSID)—and of the International Court of Justice (ICJ). The analysis discloses three main concerns when dealing with digital evidence: authorship, authenticity, and chain of custody. We propose that courts create permanent and *ad hoc* digital forensic expert committees to draft guidelines and perform a preliminary admissibility evaluation of digital evidence.

Digitalization of International Dispute Resolution

Conflicts are inherent to private and public sector activity and interactions between states in the international arena. Most states appreciate the need to value the multi-door courthouse system within their jurisdictions so that alternative dispute resolution mechanisms such as conciliation, mediation,[1] and arbitration can flourish. The same logic applies to international conflicts, where international arbitration and international mediation are effective ways to solve disputes.

Information technology is currently widely applied in justice processes. Paper-based proceedings are becoming increasingly rare, and videoconference hearings complement and replace in-person hearings.[2] Paper-based justice is rapidly being overrun by the inescapable benefits of digitalization: efficiency, accessibility, and sustainability. We are living in the digital multi-door courthouse era, that is digital dispute resolution (DDR).[3]

In the international arena, states can be involved in disputes against other states (for instance, before the ICJ, the International Tribunal for the Law of the Sea (ITLOS)), or in investment arbitration at the PCA[4]

* *Independent arbitrator, Fellow of the Chartered Institute of Arbitrators – CIArb, and Editor-in-Chief of the Revista Brasileira de Alternative Dispute Resolution - RBADR, Rio de Janeiro, Brazil.*

** *Associate professor at the Department of Business Law, Deputy Director for the International Cooperation at South Ural State University (National Research University), Chelyabinsk, Russia.*

[1] Daniel Brantes Ferreira & Luciana Severo, *Multiparty Mediation as Solution for Urban Conflicts: A Case Analysis from Brazil*, 8 BRICS L.J. 5 (2021).

[2] Daniel Brantes Ferreira, Cristiane Junqueira Giovannini, Elizaveta Aleksandrovna Gromova & Gustavo da Rocha Schmidt, *Arbitration Chambers and Trust in Technology Provider: Impacts of Trust in Technology Intermediated Dispute Resolution Proceedings*, 2 TECH. SOC'Y 101872 (2022); *see also* Daniel Brantes Ferreira, Cristiane Junqueira Giovannini, Elizaveta Aleksandrovna Gromova & Jorge Brantes Ferreira, *Arbitration Chambers and Technology: Witness Tampering and Perceived Effectiveness in Videoconferenced Dispute Resolution Proceedings*, 31 INT'L J. L. & INFO. TECH. 75 (2023).

[3] Alexey Vladimirovich Minbaleev & Kirill Sergeevich Evsikov, *Alternative Dispute Resolution in Digital Government*, 4 REVISTA BRASILEIRA DE ALTERNATIVE DISPUTE RESOLUTION – RBADR 7, 119–46 (2022).

[4] Permanent Court of Arbitration and International Court of Justice, *List of Cases* (last visited Oct. 7, 2023).

and ICSID.[5] All of these courts and tribunals admit evidence in the analog or digital form, which together comprise digitally derived evidence,[6] a concept which encompasses evidence either born digital or analog evidence later digitalized. Digital evidence is any material in the digital form used to prove a fact. It is data created, manipulated, stored, or communicated by any computer or device.[7]

To show the increasing role of digital evidence in international dispute resolution we first analyze the approaches to digital evidence applied by ICSID and the PCA. Then, we turn to the ICJ and interstate disputes.

Digital Evidence in Arbitration Institutions Involving States

Every international court or arbitration institution has specific procedural rules providing evidentiary guidelines. Consequently, judges and arbitrators hold broad discretion in evidence assessment. In any case, regardless of the evidence's form, adjudicators must reject, admit, and consider its weight (probative value) to the case.

International disputes are litigated through arbitration or in an international court.[8] There are interstate disputes and disputes filed by individuals, groups, or companies against states. Disputes involving investments between states follow a bilateral investment treaty (BIT) dispute resolution mechanism (international arbitration).[9] More commonly, investment disputes are filed before ICSID. These disputes are exclusively between states and nationals of other states.[10] ICSID excludes from its jurisdiction state-to-state disputes; these disputes are handled by the PCA.

In investment arbitration at ICSID, Rule 36(1) also gives broad discretion to the tribunal to "determine the admissibility and probative value of the evidence adduced."[11] The PCA follows the same logic in Article 27(4) of its arbitration rules, providing that the "arbitral tribunal shall determine the admissibility, relevance, materiality and weight of the evidence offered."[12] Litigants use digital evidence widely in investment arbitration both at the PCA and ICSID.

Although cases before ICSID are not interstate disputes, they demonstrate how parties can rely on digital evidence to make their case. The use of open-source evidence is more and more popular with the proliferation of social media, geographic information system (GIS, such as Google Earth or Zoom Earth), websites, and government and corporate databases. Any open-source information poses challenges for adjudicators because of its lack of consistency and reliability. In the ICSID case *Aven and Others v. Costa Rica*, the claimants (Aven and others) relied on Google Earth aerial photography to establish their argument.[13] Another example at ICSID is *Hydro and Others v. Albania*, where the claimants presented as evidence Albania's prime minister's Facebook and Twitter statements.[14]

[5] Georges R. Delaume, *ICSID Arbitration and the Courts*, 77 AJIL 784 (1983).

[6] *Introduction - Leiden Guidelines on the Use of Digitally Derived Evidence*, Leiden Guidelines on the Use of Digitally Derived Evidence.

[7] Electronic Evidence and Electronic Signatures (Stephen Mason & Daniel Seng eds., 5th ed. 2021); Daniel Brantes Ferreira & Elizaveta Alexandrovna Gromova, *Digital Evidence: The Admissibility of Leaked and Hacked Evidence in Arbitration Proceedings*, Int'l J. Semiotics L. (2023).

[8] Richard Bilder, *Adjudication: International Arbitral Tribunals and Courts*, *in* Peacemaking in International Conflict: Methods and Techniques (I. William Zartman & J. Lewis Rasmussen eds., 1997).

[9] International Institute for Sustainable Development, *Best Practices in State-to-State Dispute Settlement in Investment Treaties*.

[10] International Centre for Settlement of Investment Disputes (ICSID), Rules and Regulations.

[11] *Id.*

[12] Permanent Court of Arbitration, PCA Arbitration Rules 2012.

[13] Aven and Others v. Costa Rica, ICSID Case No. UNCT/15/3, Reply Memorial, para. 173 (Aug. 5, 2016).

[14] Hydro and Others v. Albania, ICSID Case No. ARB/15/28, Decision on Claimants' Application to Dismiss the Revision Application Under ICSID Arbitration Rule 41(5), Claimants' Request for Allocation of Advance Payments, Claimants' Requests for Security, and Respondent's Proposal for the Establishment of an Escrow Mechanism, para. 71 (Mar. 29, 2023).

https://doi.org/10.1017/aju.2024.4 Published online by Cambridge University Press

Some parties even rely on leaked diplomatic cables documents. For example, in an ICSID case, Venezuela[15] relied upon Wikileaked diplomatic cables (confidential communications between ConocoPhillips' counsel and representatives from the U.S. Embassy in Caracas).[16] In another case involving Kazakhstan, the ICSID tribunal admitted leaked e-mails as evidence adduced by the private party (Caratube International Oil Company).[17] Leaked videos were also admitted by a PCA tribunal against Canada in *Tennant Energy, LLC v. Government of Canada*.[18]

Governments produce massive amounts of digital data and are sometimes targeted by hackers or even insiders who leak documents on the web. Therefore, judges and arbitrators must apply rigorous criteria when assessing digital evidence with unknown authorship. Checking the document's authenticity is crucial in these cases. In most cases, it is the companies that uses leaked digital evidence against a state.

Digital Evidence in Interstate Disputes

There is no international law of evidence or mandatory rules on the taking of evidence (admission and evaluation), so each international court is free to design its own procedural rules. Judges and arbitrators have broad discretion in admitting and assessing evidence. The ICJ Statute provides in Article 48 that the court "shall decide the form and time in which each party must conclude its arguments and make all arrangements connected with the taking of evidence."[19] The same standard is reproduced in Article 58(2) of the Rules of Court.

In its non-binding Practice Directions III, the ICJ sets a limit on the number of pages of annexes attached by a party to a total of 750 pages, claiming that parties should adduce only "strictly selected documents."[20] Practice Direction IX*bis* provides for digital documents when referring to a "part of a publication readily available," meaning that the document should be available in public domain in any format or form or on any data medium. The page number limit implies that states must perform effective file management after e-discovery.[21] Artificial intelligence-powered document management systems can be helpful in this regard.[22]

ICJ jurisprudence has emphasized the Court's discretion to evaluate and weigh evidence.[23] In the *Democratic Republic of the Congo v. Uganda*, the Court affirmed its preference for contemporaneous evidence which can be directly confirmed, and noted that it will give more weight to evidence that did not have its authenticity challenged by impartial persons during or before the litigation.[24]

[15] ConocoPhillips Petrozuata B.V., ConocoPhillips Hamaca B.V. and ConocoPhillips Gulf of Paria B.V. v. Bolivarian Republic of Venezuela, ICSID Case No. ARB/07/30, Decision on the Proposal to Disqualify a Majority of the Tribunal, paras. 20–21 (May 5, 2015).

[16] Ferreira & Gromova, *supra* note 7.

[17] Caratube International Oil Company LLP and Devincci Salah Hourani v. Republic of Kazakhstan (II), ICSID Case No. ARB/13/13, Final Award, para. 156 (Sept. 27, 2017).

[18] Mesa Power Group LLC v. Government of Canada, PCA Case No. 2012–17, Award (Mar. 24, 2016).

[19] Statute of the International Court of Justice.

[20] International Court of Justice, Practice Directions.

[21] Esmé Shirlow, *E-Discovery in Investment Treaty Arbitration: Practice, Procedures, Challenges and Opportunities*, 11 J. Int'l Disp. Settlement 549 (Dec. 2020); *see also* Jack G. Conrad, *E-Discovery Revisited: The Need for Artificial Intelligence Beyond Information Retrieval*, 18 Artificial Intelligence L. 321 (2010).

[22] Rocío Rocha, Margarita Alonso & Angel Cobo, *Using Swarm Intelligence Techniques in Document Management Systems*, Proceedings of the Eighth International Conference on Applications of Artificial Intelligence 560 (2008).

[23] Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 ICJ Rep. 14, para. 60 (June 27).

[24] Case Concerning Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda), Judgment, 2005 ICJ Rep. 168, para. 61 (Dec. 19).

https://doi.org/10.1017/aju.2024.4 Published online by Cambridge University Press

There are several types of digital evidence adduced by states, namely digital data, videos, satellite images, and, in most recent cases, even social media material.[25] Satellite images from the internet, for example, have been adduced in recent cases because they are readily available.[26]

The Court is concerned about documents' reliability and authenticity, which plays a significant role in the assessment of digital evidence. The Court's Statute and Rules empower it to appoint experts to analyze a piece of evidence if the judge suspects it to be fraudulent. However, case law shows that the Court has adopted a passive approach in investigating the authenticity of evidence. For instance, in *Qatar v. Bahrain*,[27] after Bahrain challenged the authenticity of several documents, the Court did not rule on the matter, leaving it to the parties to reach an agreement on whether they would proceed with the documents or not. The Court's failure to rule on the matter suggests that it is reluctant to investigate suspicious digital evidence, and even to reject its admittance.

Even though the ICJ can make use of expert opinion at any time (per Article 50 of the Court's Statute), it will, like any other tribunal, usually rely on the evidence presented by the parties.[28] The Court has the power to direct the parties to produce any evidence it considers necessary, and even to seek evidence.[29] Nevertheless, it needs to act proactively to make use of these powers. For example, in *Kasikili/Sdudu Island (Botswana v. Namibia)*,[30] one judge requested satellite images of the disputed area from both states to clarify the case.

Therefore, considering the investigative power of sovereign states and the increasing availability of data and open-source surveillance technology, digital-born evidence in interstate disputes will only grow. ICJ case law corroborates this affirmation showing the increasing use by states of digital documents and audiovisual evidence such as images and videos.

When it comes to the use and evaluation of digital evidence, judges and arbitrators must take into account three vital factors: authenticity, provenance (authorship), and preservation (chain of custody).[31]

Digital Evidence Admissibility Criteria: Authenticity, Authorship, and Preservation

All domestic and international courts are attentive to the concern regarding the authenticity of digital evidence. Audiovisual material and open-source data are even more challenging than written documents. The ICJ expresses this concern in its Practice Direction IX*quater*, which addresses audiovisual and photographic material. The Practice Direction states that such evidence must be accompanied by information such as its source, circumstances and date of its making, and the date when it was publicly available. The party must also specify, if applicable, the geographic coordinates where the material was produced.[32] However, this authenticity concern conflicts with the Court's practice of admitting all the evidence presented by the parties. If the ICJ were to establish admissibility

[25] Allegations of Genocide Under the Convention on the Prevention and Punishment of the Crime of Genocide (Ukr. v. Russ.: 32 States Intervening), Public Sitting, 2023 ICJ, para. 33 (Sept. 25).

[26] Case Concerning Territorial and Maritime Dispute Between Nicaragua and Honduras in the Caribbean Sea (Nicar. v. Hond.), Judgment, 2007 ICJ Rep. 659, para. 12 (Oct. 8).

[27] Maritime Delimitation and Territorial Questions Between Qatar and Bahrain (Qatar v. Bahr.), Judgment, 2001 ICJ Rep. 40, para. 23 (Mar. 16).

[28] Marco Roscini, *Digital Evidence as a Means of Proof before the International Court of Justice*, 21 J. Conflict & Security L. 541 (2016).

[29] ICJ Statute, *supra* note 19, Arts. 49–50; ICJ Rules of Court, Art. 62.

[30] Dispute Existing Between Botswana and Namibia Concerning the Boundary Around Kasikili/Sedudu Island and the Legal Status of that Island (Kasikili/Sedudu Island – Botswana/Namibia), Judgment, 1999 ICJ Rep. 1045 (Dec. 13).

[31] Fernando Molina Granja, *The Preservation of Digital Evidence and Its Admissibility in the Court*, 9 Int'l J. Electronic Security & Digital Forensics 1 (2017).

[32] Practice Directions, *supra* note 20.

https://doi.org/10.1017/aju.2024.4 Published online by Cambridge University Press

criteria to be observed by the parties before evidence submission, this would increase reliability. Three factors are imperative: authenticity, authorship, and chain of custody.

Authenticity may be challenging to establish for evidence such as internet videos, pictures, and leaked documents. A certificate of authenticity is helpful, although in open-source internet material such as social media print screens and satellite images, the certificate will only certify the source and the date of the picture. Such a certificate might not be helpful to determine whether the evidence is trustworthy. For example, open-source aerial images are composed of a mosaic of several images collected on different dates, which can be inaccurate. The Court must be capable of stating that the evidence is sufficiently authentic and accurate to be able to be admitted. One way to evaluate authenticity would be to establish a digital forensic permanent expert committee to draft guidelines or protocols for judges so that they can know when the authenticity of a piece of evidence is questionable. Therefore, authenticity relates to reliability and accuracy.

Moreover, each tribunal should be assisted by an *ad hoc* three-member digital expert committee. One committee member would be appointed by each party and the other member by the tribunal. This dynamic preserves the committee's independence and impartiality. The Court could also accredit experts, provide an expert roster, and partner with digital experts' organizations.

The evidence's integrity is another primary concern. The documentation of the life cycle of evidence is crucial to reduce the risks of fraud. Recording every step of the data life cycle enhances its reliability and increases its probative value. The traceability and continuity of the evidence makes it possible for the expert to determine its integrity or manipulation.

Authorship is more easily established in digital documents, such as email or electronic documents, but not in digital audiovisual evidence. When the authorship is clear, the best practice is for the Court to confirm with the author during the hearing whether the evidence is authentic and the content is accurate.

In practice, international courts tend to admit even questionable evidence and then give it probative weight that corresponds with such concerns. The ICJ usually gives more probative value to written documents than to images or videos, although the latter may be vital in some cases. As the ICJ deals with states with immense digital evidence-gathering power, some guidelines and preliminary assessments should be established to admit digital evidence. Forming an expert committee for initial evaluation could be helpful for open-source and leaked digital evidence. However, case law shows that international courts including the ICJ usually wait for one of the parties to challenge a piece of evidence, which would lead, at most, to the evidence's exclusion (i.e., illegally obtained evidence). Courts do not engage in *prima facie* rejection, which would be more efficient.

Interstate disputes are complex and deal with a vast amount of digital evidence. If the ICJ remains passive in dealing with digital evidence, it will leave this topic to the judges to deal with on a case-by-case basis. Hacked and leaked evidence must be treated differently. Compliance with the clean hands doctrine is mandatory when assessing illegally obtained evidence which means that the party adducing the evidence must have not contributed with the hacking. Furthermore, the court must be cautions and confirm the authorship of leaked evidence.

Conclusion

The international arena is already digital as technology optimizes business and facilitates communication, trade, and evidence gathering. This essay showed that international courts possess broad discretion in admitting and excluding evidence, including in its digital form. At the same time, no court provides specific rules for digital evidence, so courts usually wait for the parties to challenge the evidence's authenticity before appointing an expert to evaluate it.[33]

[33] Daniel Brantes Ferreira & Elizaveta Aleksandrovna Gromova, *Electronic Evidence in Arbitration Proceedings: Empirical Analysis and Recommendations*, 20 Digital Evidence & Electronic Signature L. Rev. 30 (2023).

https://doi.org/10.1017/aju.2024.4 Published online by Cambridge University Press

We propose the creation of permanent and *ad hoc* forensic expert committees empowered to draft guidelines and perform preliminary authenticity checks in open-source and leaked evidence. Three main concerns must be borne in mind when approaching digital evidence: authenticity, provenance (authorship), and preservation (chain of custody).

https://doi.org/10.1017/aju.2024.4 Published online by Cambridge University Press