-- Journal of Criminal Law Research------
Fall 2024, 13 (48), 41-84
Jclr.atu.ac.ir
DOI: 10.22054/jclr.2025.81549.2697

ATU PRESS

Original Research
Received: 25/Aug/2024 *** Accepted: 05/May/2025
ISSN: 2345-3575
eISSN: 2476-6224

Admissibility of Digital Evidence at the International Criminal Court

Ziba Nilaei Sangari — M.A. in International Law, School of Law and Political Science, Shiraz University, Shiraz, Iran

Aghil Mohammadi* — Assistant Professor in International Law, Department of Public and International Law, School of Law and Political Science, Shiraz University, Shiraz, Iran

Abstract

Objective

Digital evidence refers to information obtained from both "closed" sources, such as USB flash drives, and "open" sources, like social media posts. This information is produced, stored, received, processed, and transmitted by digital devices. Over the past few decades, the rapid growth of information and communication technologies has enabled the generation, recording, and transmission of vast amounts of digital data. Due to its ability to capture precise timestamps and locations of events, as well as preserve information over long periods, digital evidence plays an unprecedented role in documenting international crimes. As technology advances, the International Criminal Court (ICC) encounters digital evidence more

* Corresponding Author: aghilmohammadi@shirazu.ac.ir
How to Cite: Nilaei Sangari, Z. and Mohammadi, A. (2025). Admissibility of Digital Evidence at the International Criminal Court. *Journal of Criminal Law Research,* 13(48), 41 - 84. doi: 10.22054/jclr.2025.81549.2697

frequently than its predecessors, the temporary tribunals. However, there are significant challenges in admitting digital evidence, including uncertainties regarding the motives and methods of collection, difficulties in verifying authenticity due to risks of manipulation or forgery, the lack of clarity about the source, time, and location of the data, and the potential conflict with the right to a fair trial. This article, based on a descriptive-analytical approach, examines how the ICC navigates these evidentiary materials, the associated challenges, and the court's approach to admitting digital evidence.

Methodology

This article employs a descriptive-analytical approach to examine the issue. Persian and English sources—such as books, articles, and ICC jurisprudence—were reviewed, with relevant material extracted and analyzed. Additionally, related documents, reports, and information from websites were examined to provide a comprehensive perspective on the subject.

Findings

Digital evidence is classified as documentary evidence at the International Criminal Court. Due to the unique characteristics of digital evidence, its admissibility process—based on Article 69(4) of the Rome Statute and the ICC's jurisprudence—consists of three stages: relevance, probative value, and prejudicial effect. First, the Court determines whether the evidence is prima facie relevant to the facts at issue. At the probative value stage, the Court evaluates the reliability of the evidence, considering factors like integrity, metadata, source, chain of custody, and the method of collection. In the third stage, the Court assesses whether the prejudicial effect of the evidence outweighs its probative value, ensuring the right to a fair trial is upheld. These stages are not ranked in terms of importance, as each plays a distinct role in the admissibility analysis. The Court applies a relatively low threshold when determining relevance but assesses the

significance of each piece of evidence later. In evaluating probative value, the Court focuses on factors such as reliability and the importance of the evidence for the case. The assessment of prejudicial effect is considered in light of the overall fairness of the proceedings. The Court typically excludes evidence only when its prejudicial effect significantly outweighs its probative value. The findings indicate that challenges in the admissibility of digital evidence at the ICC include uncertainties regarding the motives and methods of collection, difficulties in verifying authenticity due to manipulation risks, the obscurity of data sources, and the potential to undermine the right to a fair trial.

Novelty

This article fills the gap in scholarly attention to the legal framework governing the admissibility of digital evidence under the ICC's provisions, rules, and jurisprudence. It provides a comprehensive analysis of that framework, emphasizing both technical and legal dimensions of digital evidence. The article identifies key challenges and proposes approaches to ensure a balanced use of digital evidence at the ICC while safeguarding procedural fairness.

Conclusion

The ICC's current flexible approach to the admissibility of digital evidence is beneficial, but it is insufficient to ensure the full and effective utilization of such evidence. The ICC lacks a binding and comprehensive guideline specifically governing the assessment of digital evidence. Sole reliance on past judicial practice is inadequate to address the complexities involved in the examination and admissibility of digital evidence in future proceedings. To balance the admissibility of evidence with the right to a fair trial, the development of an official, detailed framework is essential—one that clearly articulates the technical and legal criteria applicable at each stage of the admissibility process. Additionally, the ICC should institutionalize the use of digital forensics experts and implement regular training for

judges to enhance their capacity to evaluate digital evidence. From a fair trial perspective, the ICC must ensure that defendants and their legal representatives have sufficient time and resources to challenge digital evidence effectively. Engaging experts familiar with the technical aspects of digital evidence and improving judicial understanding are vital steps. The ICC must also ensure defendants have access to qualified experts for cross-examination, safeguarding defendants' fundamental rights. Furthermore, the Court should strengthen cooperation with private entities, such as social media platforms, to preserve digital evidence, ensure access to metadata, and protect user rights.

Keywords: International Criminal Court, Digital evidence, Relevance, Probative value, Prejudicial effect, Reliability, Significance of evidence

مقاله پژوهشی

-- فصلنامه علمی پژوهش حقوق کیفری ---------
دوره ۱۳، شماره ۴۸، پاییز ۱۴۰۳، ۴۱-۸۴
Jclr.atu.ac.ir
DOI: 10.22054/jclr.2024.76302.2697

قابلیت پذیرش ادله‌ی دیجیتال در دیوان کیفری بین‌المللی

زیبا نیلائی سنگری دانش‌آموخته‌ی کارشناسی ارشد حقوق بین‌الملل، دانشکده‌ی حقوق و علوم سیاسی، دانشگاه شیراز، شیراز، ایران

عقیل محمدی * استادیار حقوق بین‌الملل، گروه حقوق عمومی و بین‌الملل، دانشکده‌ی حقوق و علوم سیاسی، دانشگاه شیراز، شیراز، ایران

تاریخ دریافت: ۱۴۰۳/۰۶/۰۴ ** تاریخ پذیرش: ۱۴۰۴/۰۲/۱۵

ISSN: ۲۳۴۵-۳۵۷۵ eISSN: ۲۴۷۶-۶۲۲۴

چکیده

ادله‌ی دیجیتال ناظر به اطلاعات برگرفته از «منابع بسته» مانند «یواس‌بی» حاوی اطلاعات و «منابع باز» مانند پست‌های بارگذاری شده در شبکه‌های اجتماعی می‌باشند که بوسیله‌ی یک دستگاه دیجیتال تولید، ذخیره، دریافت، پردازش و منتقل می‌شوند. در دادرسی‌های بین‌المللی کیفری، این ادله ظرفیت‌های مهمی جهت فرآیند تحقیق و پیگرد جرایم بین‌المللی فراهم آورده اند و سابقه‌ی استفاده از آنها به دادگاه‌های بین‌المللی کیفری موقت می‌رسد. دیوان کیفری بین‌المللی نیز از این ادله استفاده می کند. مقاله‌ی پیش‌رو مبتنی بر یک شیوه‌ی توصیفی - تحلیلی، به این سؤال پاسخ می‌دهد که فرایند پذیرش این ادله در دیوان کیفری بین‌المللی به چه نحو می‌باشد؟ با توجه به ویژگی‌های خاص ادله‌ی دیجیتال، فرایند پذیرش آنها مطابق ماده‌ی ۶۹ (۴) اساسنامه‌ی رم و رویه‌ی قضایی، شامل مراحل ارتباط، ارزش اثباتی و اثر جانبدارانه می‌باشد. نخست دیوان باید احراز کند که ادله، علی‌الظاهر به واقعیت مورد بحث در پرونده مرتبط است. در مرحله‌ی ارزش اثباتی، بصورت علی‌الظاهر مبتنی بر مؤلفه‌های قابلیت اعتماد و گاه اهمیت ادله، قابلیت ادله در اثبات چیزی که مدعی آن هستند، بررسی می‌شود. در مرحله‌ی سوم، دیوان باید قانع شود که اثر جانبدارانه‌ی ادله نقض جدی حق بر دادرسی منصفانه را به دنبال ندارد. البته مواردی چون احتمال مشخص نبودن انگیزه و روش جمع‌آوری ادله، دشواری ارزیابی اصالت ادله به دلیل جعل، مشخص نبودن منبع اطلاعات یا زمان و مکان ثبت آنها و نیز امکان تقابل ادله با حق بر دادرسی منصفانه، مهمترین چالش‌های پذیرش این ادله در دیوان هستند.

کلیدواژه ها: دیوان کیفری بین‌المللی، ادله‌ی دیجیتال، ارتباط، ارزش اثباتی، اثر جانبدارانه، قابلیت اعتماد، اهمیت ادله.

* نویسنده مسئول: aghilmohammadi@shirazu.ac.ir

مقدمه

راجع به «ادله‌ی دیجیتال»[1] مشخصاً تعریف واحدی وجود ندارد. بنابر یکی از تعاریف، ادله‌ی دیجیتال: «هرگونه اطلاعات با ارزش اثباتی است که به شکل دیجیتالی ذخیره یا منتقل می‌شود» (Avveduto et al, 2018: 174). «مرکز حقوق بشر یوسی برکلی»[2] این ادله را داده‌هایی دانسته است که: «توسط هر دستگاه، رایانه یا سیستم رایانه‌ای ایجاد، دستکاری، ذخیره یا مخابره یا از طریق یک سیستم ارتباطی منتقل می‌شوند که مرتبط با دادرسی است» (Human Rights Center UC Berkeley, 2014: 1 fn. 2) به اعتقاد «کانون وکلای بین‌المللی» نیز، ادله‌ی دیجیتال: «ادله‌ای هستند که از دستگاه‌های دیجیتال و از طریق فناوری، مانند دوربین‌ها، ماهواره‌ها و سایر فناوری‌های سنجش از دور گرفته و ایجاد شده اند» (The International Bar Association, 2016: 19). تعریف اخیر قابل قبول‌تر از سایر تعاریف به نظر می‌رسد. لذا در نهایت می‌توان گفت که ادله‌ی دیجیتال به اطلاعاتی گفته می‌شود که به وسیله‌ی دستگاه‌های دیجیتال تولید، دریافت، پردازش، ذخیره و منتقل می‌شوند و در فرایند تحقیقات و رسیدگی‌ها در دادگاه مورد استفاده قرار می‌گیرند.

ادله‌ی مذکور از «منابع بسته»[3] و «منابع باز»[4] قابل دستیابی هستند. ادله‌ی دیجیتال ناشی از منابع بسته به اطلاعاتی اشاره دارد که اختصاصی هستند و برای عموم قابل دسترس نمی‌باشند. «یواس‌بی»[5] یا دستگاه ذخیره‌سازی داده‌هایی که حاوی فیلم و عکس‌هایی است که توسط فردی ضبط شده (Kayyali et al, 2021)، نمونه‌ای از منابع بسته محسوب می‌شوند. همچنین، ادله‌ی دیجیتال را می‌توان از منابع باز و در دسترس عموم مانند تصاویر ماهواره‌ای و هوایی، پست‌های بارگذاری شده در شبکه‌های اجتماعی نیز بدست آورد. استفاده از ادله‌ی ناشی از منابع باز به دلیل ماهیت فراگیر آن، معمول‌تر از ادله‌ی ناشی از سایر منابع است.

---

1. Digital Evidence.
2. Human Rights Center UC Berkeley.
3. Closed source.
4. Open source.
5. Universal Serial Bus (USB).

سال‌هاست که در سطوح ملی و بین‌المللی، دادگاه‌ها به سمت استفاده از اطلاعات دیجیتال از جمله ادله‌ی دیجیتال در فرآیند تحقیق، تحقیب و محاکمه رفته اند. در سطح بین‌المللی، برای نمونه، دیوان بین‌المللی دادگستری در پرونده‌ی نسل‌زدایی در بوسنی به گزارش‌های سازمان ملل متحد که یافته‌هایش از جمله مبتنی بر تصاویر ماهواره‌ای بود، استناد کرد (Roscini, 2016: 549-550). در نظام بین‌المللی کیفری نیز، سابقه‌ی استفاده از ادله‌ی دیجیتال به دادگاه‌های بین‌المللی کیفری موقت همچون «نورمبرگ» و «یوگسلاوی سابق» می‌رسد و دادگاه‌های ویژه مانند «سیرالئون»[1] و «لبنان»[2] نیز از این ادله بهره برده اند.[3]

بنابر اقتضاء شرایط و پیشرفت روزافزون فناوری‌های دیجیتال، این ادله به طرز فراگیری مورد استفاده‌ی دیوان کیفری بین‌المللی قرار گرفته و می گیرند. مثلاً دیوان در سال ۲۰۱۳ میلادی در پرونده‌ی «الفقی المهدی»[4] از ادله‌ی دیجیتال همچون تصاویر ماهواره‌ای برای پیگرد جرم تخریب زیارتگاه‌ها، مساجد و اموال فرهنگی در «تیمبوکتو»[5] مالی استفاده کرد (Mimran & Weinstein, 2023). از آن زمان، بحث‌های زیادی در مورد نیاز به گنجاندن بیشتر ادله‌ی دیجیتال در فرایندهای نظام بین‌الملل کیفری مطرح شد. در حال حاضر نیز استفاده از ادله‌ی دیجیتال همچون تصاویر ماهواره‌ای و هوایی برای مستندسازی

1. Special Court for Sierra Leone (SCSL).
2. Special Tribunal for Lebanon (STL).
۳. برای مثال، در دادگاه نورمبرگ، ادله‌ی دیجیتالی همچون فیلم‌ها برای اثبات جنایات رخ داده شده توسط نازی‌ها در دادگاه مزبور اجازه اکران یافتند ("Trial of the Major War Criminals Before the International Military Tribunal (Nuremberg: International Military Tribunal", 1947, p. 169-171). همچنین دادگاه یوگسلاوی سابق در پرونده‌هایی همچون پرونده‌ی «تولیمیر» از ادله‌ای همچون فیلم‌ها و تصاویر هوایی استفاده کرد (IT-05-88/2-T, 12 December 2012, para. 592-594). دادگاه سیرالئون از کلیپ‌های صوتی در پرونده‌ی «چارلز تیلور» بهره برد (SCSL-03-01-T-745, 25 February 2009, paras. 4-7). در پرونده‌ی سلیم جمیل عیاش در دادگاه ویژه‌ی لبنان نیز ادله‌ی دیجیتال مهمی همچون ارتباطات رهگیری شده مورد استفاده قرار گرفت (STL-11-01/T/TC, 31 October 2016, paras. 23-25).
4. Al Faqi Al Mahdi.
5. Timbuktu.

جرایم رخ داده در پرونده‌ی مخاصمه‌ی روسیه و اوکراین در دیوان نیز ادامه دارد (Niezen, 2023).

چالش‌های استفاده از این ادله همچون حجم زیاد داده‌ها و پیچیده بودن تحلیل فنی آن‌ها، در معرض تغییر، جعل و انگیزه‌ی مغرضانه بودن یا گاه مشخص نبودن پدیدآورنده‌ی آنها نباید باعث چشم‌پوشی از ظرفیت‌های آن شود. ادله‌ی دیجیتال در مواردی که تحقیقات بین‌المللی کیفری با موانع قانونی و سیاسی روبه‌رو است، اهمیت‌شان بیشتر به چشم می‌آید. مثلاً در مواردی که دادستان یا بازرسان دیوان کیفری بین‌المللی برای ورود به یک منطقه‌ی جغرافیایی با مانع یا محدودیت‌هایی از سوی دولت میزبان مواجه می‌شوند (Stavrou, 2021). دسترسی گسترده به موبایل و اینترنت، امکان ثبت جرایم بین‌المللی و انجام تحقیقات بیشتر را فراهم می‌آورد، زیرا اطلاعات دیجیتال همچون تصاویر و فیلم‌ها اغلب می‌توانند به پرسش‌هایی مهمی همانند «چه موقع»، «کجا» و «چه کسی» پاسخ دهند و داده‌های زمانی و مکانی مهمی را ارائه دهند یا اینکه اطلاعاتی در خصوص اینکه چه کسی مرتکب جرم شده و چه کسی قربانی بوده است را تأمین کنند (Freeman, 2019: 59). مثلاً دادگاه بین‌المللی کیفری یوگسلاوی سابق از «ارتباطات شنود شده» بعنوان شواهدی برای اثبات کشتار «سربرنیتسا»[1] استفاده کرده است (Ragni, 2023: 5). همچنین دادستان دادگاه ویژه‌ی لبنان از جمله به داده‌های جغرافیایی و داده‌های تلفن همراه مانند سوابق تماس‌ها استناد کرد تا بتواند اثبات کند که متهمان، از حادثه‌ی ترور «رفیق حریری»[2] نخست‌وزیر وقت لبنان و ۲۱ نفر دیگر در بیروت در ۱۴ فوریه ۲۰۰۵ اطلاع داشته و آن را برنامه‌ریزی کرده بودند (Freeman & Vazquez Llorente, 2021: 177-178).

ظرفیت مهم دیگری که می‌توان برای ادله‌ی دیجیتال برشمرد، در مقایسه با ادله‌ی سنتی مشخص می‌شود. بسیاری از انواع ادله‌ی سنتی با اینکه در معرض از بین رفتن در طول زمان هستند، اما در سطح تحقیقات ملّی به دلیل امکان بازدیدِ غالباً به موقع از صحنه‌های جرم، تا حد زیادی حفظ می‌شوند. این در حالی است که در صورت وقوع جرایم بین‌المللی،

1. Srebrenica.
2. Rafik Hariri.

فرآیند تحقیقات ممکن است سال‌ها طول بکشد و در طی زمان، ادله‌ی سنتی از بین بروند. در مقابل، ادله‌ی دیجیتال به دلیل اینکه به آسانی در پلتفرم‌های آنلاین حفظ می‌شوند و از یک دستگاه به دستگاه دیگر منتقل می‌شوند، کمتر در معرض محدودیت مذکور قرار دارند (Hellwig, 2022: 974, 976).

ظرفیت دیگر ادله‌ی دیجیتال این است که باعث می‌شوند که جامعه‌ی مدنی نقش فعالی در فرآیند جمع‌آوری ادله ایفاء کند. در این خصوص، یکی از اقدامات ارزشمند «دفتر دادستانی»[1] دیوان کیفری بین‌المللی، راه‌اندازی پلتفرم آنلاین «OTPLink»[2] در ماه مه ۲۰۲۳ میلادی بود. این پلتفرم به قربانیان، شاهدان، سازمان‌های مردم‌نهاد غیردولتی و سایرین این امکان را می‌دهد تا مدارک مربوط به جنایات بین‌المللی را بصورت دیجیتال به دفتر دادستانی ارسال کنند. این پلتفرم توانسته واسطه‌ها برای ارتباط با آسیب‌دیدگان را تا حدی کم کند؛ واسطه‌هایی که ممکن است دیدگاه‌های آسیب‌دیدگان را بطور نادرست انتقال دهند یا به مشارکت بزهدیدگان آسیب بزنند (Mimran & Weinstein, 2023).

با توجه به ظرفیت‌های چشمگیر ادله‌ی دیجیتال در اثبات حقیقت و کمک به تحقق عدالت بین‌المللی کیفری، بهره‌گیری مؤثر از این ظرفیت‌ها مستلزم آن است که ادله‌ی دیجیتال مطابق استانداردهای دیوان بین‌المللی کیفری، پذیرفته شوند. این امر، ضرورت بررسی مراحل پذیرش ادله‌ی مزبور را بیش از پیش نمایان می‌سازد. نظر به این موضوع، این مقاله بر اساس یک شیوه‌ی توصیفی - تحلیلی، به این سؤال پاسخ می‌دهد که فرایند پذیرش این ادله در دیوان کیفری بین‌المللی به چه نحو می‌باشد؟ قابلیت پذیرش ادله در رسیدگی‌های بین‌المللی کیفری در قاعده‌ی ۶۴ آیین دادرسی و ادله و بطور ویژه‌تر و دقیق‌تری در ماده‌ی ۶۹ (۴) اساسنامه‌ی رم ذکر شده است. ماده‌ی ۶۹ (۴) اساسنامه‌ی رم شامل یک آزمون سه مرحله‌ای برای پذیرش ادله بطور کلی می‌باشد که بنابر رویه‌ی قضایی دیوان، به ادله‌ی دیجیتال هم تسری می‌یابد. مطابق این مقرره: «دیوان می‌تواند مطابق آیین دادرسی و ادله، در مورد مرتبط بودن یا قابل پذیرش بودن هر مدرکی، از جمله ارزش اثباتی مدرک و هر گونه خدشه‌ای که ممکن است چنین مدرکی به دادرسی منصفانه یا

1. Office of the Prosecutor (OTP).
2. https://otplink.icc-cpi.int/.

ارزیابی منصفانه‌ی شهادت شهود بزند، تصمیم بگیرد».[1] این مراحل شامل مراحل ارتباط، ارزش اثباتی و اثر جانبدارنه می‌باشند. البته دیوان با در نظر گرفتن ماهیت خاص و ویژگی‌هایی که این ادله دارند، برای آزمون هر یک از این مراحل، مؤلفه‌های مهمی را دخیل می‌داند.

شایان ذکر است که آثار بسیار اندکی در زمینه‌ی چارچوب حقوقی پذیرش ادله‌ی دیجیتال منتشر شده و تاکنون هیچ پژوهشی بطور خاص راجع به پذیرش ادله‌ی دیجیتال با توجه به قوانین، قواعد و رویه‌های دیوان کیفری بین‌المللی صورت نگرفته است. در میان آثار فارسی، علی‌رغم اینکه مثلاً مقاله‌ی «ارزیابی اصالت ادله‌ی الکترونیکی و ارزش اثباتی آن‌ها» (السان و منوچهری (۱۳۹۷)، به نکات مهمی در خصوص ارزش اثباتی ادله‌ی الکترونیکی، قلمرو اعتبار ادله‌ی الکترونیکی، اصالت و قابلیت اعتماد ادله‌ی مذکور اشاره داشته و به مطالعه‌ی تطبیقی نظام حقوقی ایران، مقررات آنسیترال، رویه‌ی قضایی و داوری کشورهای آمریکا و انگلستان پرداخته است، اما این اثر چارچوب حقوقی پذیرش ادله‌ی دیجیتال در دیوان کیفری بین‌المللی را بررسی نکرده است.

همچنین جلالی فراهانی (۱۳۸۶) در مقاله‌ی «استنادپذیری ادله‌ی الکترونیکی در امور کیفری»، نقاط قوت و ضعف داده‌های الکترونیکی، قواعد ناظر بر استنادپذیری ادله‌ی الکترونیکی و قواعد حقوقی ناظر بر اقدامات مجریان قانون در مواجهه‌ی با ادله‌ی مذکور را در چارچوب نظام حقوقی ایران بررسی کرده است. با اینکه مطالب این مقاله در باب ماهیت ادله‌ی الکترونیکی و بعضی مؤلفه‌های مورد اشاره در خصوص استنادپذیری ادله در نگارش مقاله حاضر کمک خواهند کرد، اما نویسنده بصورت خاص به ادله‌ی دیجیتال در چارچوب دیوان کیفری بین‌المللی نپرداخته است، مقاله‌ی «تحلیلی بر نحوه‌ی ارائه‌ی ادله و استنادپذیری داده‌های سنجش از راه دور در محاکم بین‌المللی» به نویسندگی توحیدی و افضل‌پور (۱۳۹۹) به بررسی سنجش از راه دور بعنوان یکی از انواع ادله‌ی دیجیتال در دیوان بین‌المللی دادگستری و دیوان بین‌المللی حقوق دریاها پرداخته است و اگرچه نکات آن در خصوص راهکارهای مواجهه با سنجش از راه دور برای پژوهش

1. Rome Statute of the International Criminal Court, 1998, Art. 69(4).

حاضر مفید می‌باشد، اما مقاله مزبور هیچ‌گونه اشاره‌ای به چارچوب حقوقی پذیرش ادله‌ی دیجیتال در دیوان کیفری بین‌المللی نداشته و در خصوص ادله‌ی دیجیتال نیز صرفا سنجش از راه دور را مدنظر داشته است. در مجموع نظر به توضیحات فوق باید گفت که با توجه به نبود یک اثر خاص در خصوص چارچوب حقوقی پذیرش ادله‌ی دیجیتال در دیوان کیفری بین‌المللی، مقاله‌ی پیش رو تلاش کرده است مطالب جدید و نوآورانه‌ای به مخاصب عرضه دارد.

حال با توجه به آنچه گفته شد، این مقاله در راستای تبیین چارچوب حقوقی پذیرش ادله‌ی دیجیتال در دیوان کیفری بین‌المللی، مراحل سه‌گانه‌ی ارتباط، ارزش اثباتی و اثر جانبدارانه را در سه قسمت بررسی خواهد کرد.

۱. ارتباط

مرحله‌ی اول برای ارزیابی و پذیرش ادله در دیوان، «ارتباط»[1] یا مرتبط بودن ادله بصورت «علی‌الظاهر»[2] می‌باشد. طبق بند ۴ ماده‌ی ۶۹: «دیوان می‌تواند در مورد مرتبط بودن یا قابل پذیرش بودن هر مدرکی ... تصمیم بگیرد». در قاعده‌ی ۶۴ (۳) آیین دادرسی و ادله‌ی دیوان نیز مقرر شده است: «ادله‌ای که حکم به غیرقابل پذیرش بودن یا نامرتبط بودن آن شود، نبایستی توسط شعبه در نظر گرفته شود». در خصوص مؤلفه‌ی ارتباط، شعبه‌ی دوم محاکمه در پرونده‌ی «کاتانگا»[3] اشعار داشته است که: «ادله در صورتی مرتبط قلمداد می‌شوند که وجود یک واقعیت مورد بحث را کم و بیش محتمل کنند و اینکه آیا آن مدرک مرتبط است یا خیر، بستگی به هدفی دارد که مدرک بر اساس آن ارائه شده است» (ICC-01/04-01/07, 2010, para. 16). بنابر نکات مزبور مشخص می‌شود که یک مدرک دیجیتال باید نشان دهد که چگونه یک واقعیت مشخص به یکی از موضوعات اساسی پرونده ارتباط دارد و چرا این ارتباط برای کشف حقیقت مهم است. همچنین باید نشان دهد که مدرک ارائه شده چگونه بر احتمال وقوع آن واقعیت اثر می‌گذارد. به بیان

1. Relevance.
2. Prima facie.
3. Katanga.

دیگر، مدرک باید به گونه‌ای باشد که باور به آن واقعیت را منطقی‌تر و محتمل‌تر کند. با این حال، اگر مدرک دیجیتال به‌گونه‌ای باشد که احتمال وقوع آن واقعیت را کمتر محتمل کند، باز هم می‌تواند مرتبط محسوب شود، زیرا همچنان بر ارزیابی واقعیات پرونده تأثیر دارد. در نتیجه، معیار ارتباط مدرک، توانایی آن در تغییر احتمال وقوع یک واقعیت است، چه این تغییر به سمت بیشتر محتمل شدن واقعیت باشد و چه به سمت کمتر محتمل شدن آن.

نظر به این دیدگاه می‌توان گفت که مرحله‌ی ارتباط، هم یک مبنای قانونی برای حذف ادله‌ی نامرتبط با رسیدگی است و هم هدف یک مدرک را در دادرسی تعیین می‌کند. مثلاً هنگام ارزیابی عنصر ارتباطِ یک فیلم در رسانه‌های اجتماعی، این موضوع بایستی در نظر گرفته شود که تمام یا بخشی از اطلاعات فیلم مربوط چه نقش و ارتباطی در اثبات یا رد واقعیت‌های مورد بحث در یک پرونده‌ی خاص دارد. البته برای اینکه مدرکی، مرتبط در نظر گرفته شود، لزومی ندارد که صرفاً و بطور خاص به وقایع مورد بررسی دیوان بپردازد، بلکه همین که بصورت کلی به پرونده مربوط باشد، برای مرتبط تلقی شدن کفایت می‌کند (Laving, 2014: 18-19). در این خصوص، پرونده‌ی «بِمبا»[1] مثال خوبی است. جنبش آزادی‌بخش کنگو به فرماندهی بمبا، در جریان سرکوب کودتا علیه دولت مرکزی در جمهوری آفریقای مرکزی (۲۰۰۲-۲۰۰۳) جنایات علیه بشریت و جنگی متعددی را مرتکب شدند. دیوان در جریان بررسی پرونده و صدور حکم بازداشت برای بمبا در سال ۲۰۰۸، برای اثبات آگاهی بمبا از جرایم رخ داده توسط جنبش به «گزارش سازمان ملل متحد»[2]راجع به جنایات ارتکابی توسط این جنبش در «مامباسا»[3]کنگو (دسامبر ۲۰۰۲ – ژانویه ۲۰۰۳) استناد کرد. دادستان نیز در خصوص اتهامات مطرح علیه بمبا، بطور گسترده در مورد رفتار جنبش مزبور در مامباسا بحث کرد. در واقع، اگرچه بمبا متهم به ارتکاب جنایت در آفریقای مرکزی بود، اما دادستان به رفتار جنبش در مامباسا استناد کرد تا نشان بدهد که بمبا باید می‌دانست که این جنبش وقتی که به آفریقای مرکزی اعزام می‌شوند،

1. Jean-Pierre Bemba Gombo.
2. Human Rights Watch., “ICC: Q&A on the Trial of Jean-Pierre Bemba”, 2010.
3. Mambasa.

مرتکب جنایاتی در آن منطقه خواهند شد. نکته‌ی مهم این پرونده این است دیوان در پاسخ به اعتراض متهم به عدم ارتباط گزارش سازمان ملل با اتهامات مطروحه، اظهار داشت که اگرچه گزارش مزبور به جنایات رخ داده در سرزمینی غیر از آفریقای مرکزی اشاره دارد، اما اقدامات جنبش در همان برهه‌ی زمانی‌ای (۲۰۰۲-۲۰۰۳) اتفاق افتاده که بمبا نیز مرتکب جنایت شده است. همچنین اذعان داشت که اطلاعات مربوط به اقدامات جنبش در مامباسا می‌تواند اطلاعاتی مرتبط با وقایع پرونده همچون نقش بمبا در اقدامات نظامی جنبش در آفریقای مرکزی و قصد او، تعیین توانایی و اختیارات او برای اعمال اقدامات انضباطی و جلوگیری از جرایم رخ داده را مشخص کند (ICC-01/05-01/08, 2013, paras. 12-13). این مثال نشان می‌دهد که «مرحله‌ی ارتباط» می‌تواند شامل ارتباط غیرمستقیم مدرک با موضوع پرونده باشد و نه فقط ارتباط مستقیم. در واقع، دیوان گزارش سازمان ملل متحد را بعنوان یک مدرک مربوط صرفاً به دلیل اینکه به آفریقای جنوبی مرتبط نبود، نادیده نگرفت، بلکه به قسمت‌های مرتبط آن با جنبه‌های مختلف پرونده‌ی بمبا و همچنین محدوده‌ی زمانی جرایم رخ داده و تهیه‌ی گزارش مزبور توجه کرد.

به نظر می‌رسد رویکرد دیوان در قضیه‌ی فوق در خصوص احراز عنصر ارتباطِ یک مدرک به پرونده، قابل تعمیم به ادله‌ی دیجیتال نیز باشد. ادله‌ی دیجیتال همچون عکس‌ها و فیلم‌ها حاوی اطلاعات بسیاری هستند و ممکن است عکس یا فیلمی با محدوده‌ی زمانی منطبق با موارد تحت رسیدگی در دیوان ارائه شود که بخشی از اطلاعات آن، غیرمرتبط و بخش دیگر، مرتبط با سایر جهات مختلف پرونده باشد، اما مستقیماً به وقایع مورد بحث دیوان نپردازد. در این حالت نیز دیوان صرفاً به خاطر نامرتبط بودن بخشی از مدرک به پرونده، کلاً آن را کنار نخواهد گذاشت و از بخش‌های مرتبط آن ولو بصورت غیرمستقیم برای سایر جهات مرتبط پرونده استفاده خواهد کرد.

مطلب مهم دیگر در خصوص عنصر ارتباط، اینکه به نظر می‌رسد با توجه به اینکه دیوان صلاحیت رسیدگی به جدی‌ترین جنایاتی که مایه‌ی نگرانی جامعه‌ی بین‌المللی است را دارد، ضرورت دارد که برای تحقیق، تعقیب و محاکمه مؤثرتر، رویکرد گسترده‌تری جهت مرتبط قلمداد کردن ادله‌ی دیجیتال داشته باشد. ظاهراً در عمل نیز رویه‌ی دیوان

نشان از این دارد که بسیاری از ادله، مرتبط در نظر گرفته می‌شوند. با این حال، نباید از نظر دور داشت که پذیرش ادله‌ی دیجیتال نامرتبط ممکن است بر روند دادرسی منصفانه اثر منفی نیز داشته باشد. در این خصوص، می‌توان اشاره کرد که بعنوان مثال، اگر دادستان قصد دارد از سوابق داده‌های تماس‌هایی خاص و آدرس «آی پی»[1]آن‌ها برای دانستن این نکته که تماس‌ها از کجا انجام شده اند، استفاده کند و آن را تحت عنوان مدارک مرتبط، به دیوان ارائه دهد، متهم و وکلای او باید به سوابق تماس‌ها و همچنین روش مورد استفاده دفتر دادستانی برای جمع‌آوری اطلاعات مربوط دسترسی داشته باشند تا چنانچه معتقد به غیرمرتبط بودن آنها هستند، بتوانند از خود دفاع کنند (Arcos Tejerizo, 2023: 756). در غیر این صورت اصل «تساوی سلاح‌ها»[2]و به تبع آن حق به چالش کشیدن ادله، نقض و به روند دادرسی منصفانه خدشه وارد خواهد شد. نکته‌ی دیگر اینکه چون ادله‌ی دیجیتال و فراداده‌ها به نسبت ادله‌ی سنتی، بیشتر در معرض جعل و تغییر قرار دارند، قضات بایستی از ارزش فراداده‌ها و اینکه به چه دلیل اطلاعات داده‌های مذکور مربوط به یک پرونده‌ی جنایی است، آگاه باشند، زیرا عدم آگاهی از مفاهیمی همچون فراداده‌ها می‌تواند توانایی دادگاه را در مواجهه‌ی با ادله‌ی دیجیتال کاهش دهد (Braga da Silva, 2021: 80 / Janfalk, 2021: 80).

مشخص بودن تاریخ ادله‌ی دیجیتال نیز نقش مهمی در مرتبط قلمداد شدن یا نشدن ادله ایفاء می‌کند. در این خصوص، دیوان در پرونده‌ی «کاتانگا» بیان داشته است که احراز عنصر ارتباط راجع به ادله‌ای همچون فیلم‌ها، عکس‌ها و صداهای ضبط شده، به تاریخ یا محل ضبط بستگی دارد و باید ادله‌ای در این زمینه ارائه شود (ICC-01/04-01/07, 2010, para. 24). نکته‌ی مهم دیگر در خصوص مرحله‌ی ارتباط، اینکه جز در مواردی که دیوان می‌تواند فوراً مرتبط بودن را از خود مدرک تشخیص دهد، اثبات ارتباط اطلاعات ارائه شده با یک واقعیت سرنوشت‌ساز در پرونده، بر دوش ارائه‌دهنده‌ی مدرک

1. Internet Protocol (IP).
2. Equality of arms.
این مفهوم مستلزم وجود تعادل منصفانه بین فرصت‌هایی است که برای طرفین دعوا در نظر گرفته شده است. مثلاً طرفین باید بتوانند شهود خود را احضار کنند و ضمناً قادر باشند شهود طرف مقابل را مورد پرسش قرار بدهند.

خواهد بود و او است که باید توضیح دهد که اطلاعات موجود در ادله‌ی ارائه شده چگونه واقعیت‌های موجود در پرونده را محتمل‌تر یا کمتر محتمل می‌کند (ICC-01/04-01/07, 2010, para. 16). شایان توجه است که اگرچه صرف مرتبط بودنِ علی‌الظاهر ادله، قابل پذیرش بودن آن‌ها را تضمین نمی‌کند، اما درصورت نامرتبط قلمداد شدن یک مدرک، عملاً آن مدرک رد می‌شود و دادگاه دیگر به سراغ آزمون و احراز مراحل دوم و سوم پذیرش مدرک یعنی ارزش اثباتی و اثر جانبدارانه در برابر ارزش اثباتی نخواهد رفت.

۲. ارزش اثباتی ادله‌ی دیجیتال و مؤلفه‌های آن

«ارزش اثباتی»[1] دومین مرحله‌ی آزمون پذیرش ادله‌ی دیجیتال می‌باشد. بند ۴ ماده‌ی ۶۹ مقرر می‌دارد که: «دیوان می‌تواند ... در مورد مرتبط بودن یا قابل پذیرش بودن هر مدرکی، از جمله ارزش اثباتی ... تصمیم بگیرد». در این مرحله، این احتمال سنجیده می‌شود که آیا ادله‌ی ارائه شده بر تعیین و اثبات یک واقعیت اثر دارند یا خیر (Quilling, 2022). با اینکه اساسنامه و آیین دادرسی دادگاه‌های کیفری بین‌المللی از جمله دیوان کیفری بین‌المللی به این مرحله اشاره دارند، اما فهرست قطعی از عناصر و مؤلفه‌های آن ارائه نکرده اند و تفسیر عناصر مؤثر در ارزیابی ارزش اثباتی آن‌ها هم در میان قضات متفاوت بوده و قواعد ثابت و روشنی در قوانین دادگاه برای این موضوع تدوین نشده است. به همین دلیل، تحلیل رویه‌ی قضایی دیوان و بررسی تصمیمات صادره در پرونده‌های مختلف برای درک عوامل مؤثر در ارزیابی ارزش اثباتی ادله ضروری است.

بررسی این رویه‌ها نشان می‌دهد که نحوه‌ی ارزیابی دیوان در پرونده‌های گوناگون متنوع بوده و قاعده‌ای یکسان و جامع برای تمامی پرونده‌ها وجود ندارد. با این حال، در این میان، پرونده‌ی «کاتانگا»[2] بعنوان یک نمونه‌ی برجسته شناخته می‌شود که ساختار ارزیابی ارزش اثباتی ادله‌ی مستند را بصورت کامل‌تر و منطقی‌تر تبیین کرده است و از آنجا که در پرونده‌ی مزبور، دیوان ادله‌ی دیجیتال را بخشی از ادله‌ی مستند می‌داند، این

1. Probative value.
2. Katanga.

چارچوب برای تحلیل ارزش اثباتی ادله‌ی دیجیتال نیز قابل استفاده است. در این پرونده، از مؤلفه‌های «قابلیت اعتماد»[1] و «اهمیت ادله»[2] که هر کدام، شاخص مختلفی را شامل می‌شود، برای تجزیه و تحلیل ارزش اثباتی ادله‌ی دیجیتال استفاده شده است. مؤلفه‌ی قابلیت اعتماد شامل عواملی مانند اصالت و سایر نشانه‌های قابلیت اعتماد است که در تمامی پرونده‌هایی که ادله‌ی دیجیتال بررسی شده است، با توجه به نوع و ویژگی‌های خاص هر ادله، از موارد مرتبط آن برای ارزیابی ارزش اثباتی بهره‌برداری شده است. اما مؤلفه‌ی اهمیت ادله که در پرونده‌ی کاتانگا صراحتاً مورد تأکید قرار گرفته، در برخی پرونده‌های دیگر مستقیماً ذکر نشده است. از این رو، دلیل تمرکز بر چارچوب ارائه‌شده در پرونده‌ی فوق، ساختار منطقی و منسجم آن در ارزیابی ارزش اثباتی ادله‌ی مستند است که از عناصر قابلیت اعتماد و اهمیت ادله بصورت هم‌زمان بهره می‌گیرد. در ادامه، دو مؤلفه‌ی مذکور مورد بررسی و تحلیل قرار می‌گیرند.

۲-۱. قابلیت اعتماد

در خصوص مؤلفه‌ی «قابلیت اعتماد» ادله، نظر دادگاه کیفری بین‌المللی یوگسلاوی سابق این است که ادله باید «داوطلبانه»[3]، «صادقانه»[4] و «موثق»[5] باشند (Prosecutor v. Zlatko Aleksovski, 1999: para.15). در واقع، این مؤلفه ناظر به این مسئله است که آیا یک مدرک و اطلاعات آن، همان چیزی است که مدعی اثبات آن است یا خیر. بنابر رویه‌ی

1. Reliability.
2. Significance of evidence.
3. Voluntary.

به این معناست که مدرک باید بدون اجبار، تهدید یا فریب به دست آمده باشد. وقتی فردی بصورت داوطلبانه اطلاعاتی ارائه می‌دهد، احتمال بیشتری وجود دارد که آن اطلاعات صادقانه و مطابق با واقعیت و به تبع آن قابل اعتماد باشد. در مقابل، اگر مدرک تحت اجبار یا فریب به دست بیاید، غیر قابل اعتماد خواهد بود چون فرد ممکن است صرفاً برای رهایی از فشار، اطلاعات نادرستی را ارائه دهد.

4. Truthful.
5. Trustworthy.

قضایی، قابلیت اعتماد یک مدرک از طریق شاخص «اصالت»[1] و «سایر شاخص‌های قابلیت اعتماد»[2] سنجیده می‌شود که در ادامه تبیین می‌شوند.

۲-۱-۱. اصالت

اولین اقدام دیوان در ارزیابی قابل اعتماد بودن یک مدرک، اصالت‌سنجی یا احراز هویت آن می‌باشد که هدف آن، حصول اطمینان از اصالت مدرک، عدم تغییر و جعل ادله‌ی دیجیتال می‌باشد (Ashouri et al, 2014: 4). لازم به ذکر است که هر دو واژه‌ی اصالت‌سنجی یا هویت‌سنجی به معنای شناسایی و تصدیق هویت واقعی فرد در دنیای واقعی یا مجازی به کار می‌روند. هویت در لغت به معنای حقیقت یا جوهره‌ای است که مجموعه‌ای از ویژگی‌های اساسی یک موجود را تشکیل می‌دهد. در این راستا، اصالت‌سنجی یا احراز هویت به فرایندی اطلاق می‌شود که در آن ویژگی‌های خاص و مشخص یک فرد یا موجود بطور قطعی تأیید می‌شود تا اطمینان حاصل گردد که آن ویژگی‌ها به همان موجود تعلق دارند. این روند در دنیای دیجیتال و سیستم‌های اطلاعاتی بطور فزاینده‌ای مهم و ضروری شده است. در سیستم‌های الکترونیکی، تأیید هویت معمولاً شامل بررسی ویژگی‌هایی همچون نام و نشانی است که بعنوان ارکان اساسی شناسایی فرد پدیدآورنده‌ی اطلاعات دیجیتال در نظر گرفته می‌شوند (فیضی چکاب، ۱۳۸۹: ۱۹۵).

در این خصوص چالش‌هایی در مواجهه با اصالت‌سنجی ادله‌ی دیجیتال وجود دارد؛ از جمله اینکه اسناد دیجیتال گاهی به راحتی قابل تغییرند. برای مثال، اگر یک سند دیجیتالی بصورت ایمیل ارسال شود، ممکن است با استفاده از ابزارهای فنی، اصلاحاتی در محتوای آن اعمال گردد. البته چنین تغییراتی معمولاً قابل شناسایی هستند و کارشناسان فناوری اطلاعات می‌توانند زمان و نوع تغییرات را تشخیص دهند. با وجود این، همین امکان تغییر در اسناد دیجیتال باعث می‌شود که افراد بتوانند از نظر قانونی، ادعاهایی مانند جعل، انکار یا تردید درباره‌ی اعتبار این اسناد را مطرح کنند (روح‌بخش، ۱۴۰۲: ۱۵۳).

---

1. Authentication.
2. Other criteria of reliability.

در همین راستا مهم است که اشاره شود که در خصوص ادله‌ی دیجیتال، با توجه به اینکه در عصر اطلاعات می‌توان از طریق فناوری «جعل عمیق»[1] فیلم‌ها و عکس‌هایی را به وجود آورد که تشخیص واقعی یا ساختگی بودن آن‌ها با مشکلات فراوانی روبه‌رو باشد، مسئله‌ی اصالت‌سنجی اطلاعات دیجیتال بسیار حائز اهمیت خواهد شد (Lane, 2021). البته دیوان مقرر نمی‌کند که اصالت ادله بصورت رسمی یا توسط شاهد در دیوان اثبات شود. در واقع، دیوان برای اصالت‌سنجی ادله‌ی دیجیتال بیان می‌کند که ادله یا بایستی خود-اصالت‌سنج باشند، یا طرفین پرونده بر اصالت آن توافق کرده باشند، یا نشانه‌های کافی از قابل اعتماد بودن را برآورده سازند و یا اگر نشانه‌های کافی بر قابل اعتماد بودن آن وجود نداشته باشد باید طرفی که مدرک را ارائه می‌دهد اطلاعاتی دال بر اصالت و قابل اعتماد بودن آن به شعبه ارائه دهد به نحوی که شعبه بتواند اصالت آن را بررسی نماید (ICC-01/05-01/08, 2012: para. 9).

«اصالت منشأ»[2] «یکپارچگی / تمامیت»[3] تاریخ و محل ثبت اطلاعات، هویت پدیدآورنده‌ی اطلاعات و «زنجیره‌ی نگهداری»[4] و «حفظ»[5] ادله (ICTR-98-44-T, 2008: para. 22)، معیارهای بررسی اصالت اولیه‌ی یک مدرک دیجیتال می‌باشند. با این حال، چون یکی از ویژگی‌های خاص فناوری اطلاعات و ارتباطات، ناشناختگی می‌باشد، ممکن است انتساب فعل به پدیدآورنده‌ی دیجیتال به آسانی میسر نباشد (مؤذن‌زادگان و شایگان، ۱۳۸۸: ۸۷) چراکه در اینترنت، کاربران می‌توانند ناشناس بمانند که این امر اثبات ارتباط داده‌ها با هویت واقعی را دشوار می‌کند. این موضوع در مسائل مختلفی بویژه در جرایم سایبری و گفتگوهای آنلاین اهمیت دارد، زیرا می‌توان برای اثبات

---

1. Deep Fake.
جعل عمیق نوعی هوش مصنوعی است که می‌تواند محتوای تصاویر، فایل‌های ویدئویی و صوتی را به گونه‌ای تغییر دهد که محتوای جدیدی تولید شود.

2. Originality.
3. Integrity.
یکپارچگی به معنای عدم تغییر و منقطع نشدن ادله می‌باشد. مثلاً یک صوت یا مصاحبه‌ی تصویری باید بصورت کامل ارائه شود، نه اینکه مشخص شود که بخشی از آن حذف شده است.

4. Chain of custody.
5. Preservation.

جرایم رخ داده، به اعتراف فرد در مکالمات، وجود اطلاعات شخصی مرتبط و شواهد فنی در سخت‌افزار استناد کرد. در این باره، از چالش‌های مهم ادله‌ی مزبور، استفاده از نام‌های مستعار و اطلاعات جعلی است که احراز اصالت یا هویت‌سنجی ادله‌ی دیجیتال را پیچیده‌تر هم می‌کند (داودی‌بیرق، ۱۳۸۷: ۱۰۵). مثلاً زمانی که متنی در یک محیط داده‌پردازِ دیجیتال همانند رایانه نوشته می‌شود، در اکثر اوقات فقط به یک شیوه‌ی نگارش دسترسی وجود دارد که صرفاً با مطالعه‌ی متن و بررسی نحوه‌ی نگارش آن نمی‌توان به هویت پدیدآورنده‌ی سند پی برد، زیرا هر کاربری که با فناوری مذکور آشنا باشد، می‌تواند آن مطالب را نوشته باشد. البته اگرچه اسنادی که در یک محیط داده‌پرداز ایجاد شده است، معمولاً به نام کسی است که نامش به هنگام نصب برنامه درج شده است، ولی چنین اطلاعاتی با اینکه سازنده است، اما کافی و اطمینان‌بخش نیست، زیرا یک سیستم رایانه‌ای می‌تواند برای افراد زیادی قابل دسترس باشد (حیدری، ۱۴۰۰: ۸-۹).

با این حال، ادله‌ی دیجیتال در دیوان را می‌توان از طریق شاخص‌های خارجی مانند شهادتِ ترجیحاً شاهد مستقیم، اشخاص حرفه‌ای، کارشناسان و همچنین شناسایی منبع آن یا از طریق شاخص‌های داخلی همانند بررسی فراداده‌ی ادله‌ی دیجیتال اصالت‌سنجی کرد (Ashouri et al, 2014: 5). در این رابطه لازم به ذکر است که برخی از ادله‌ی دیجیتال نیز اصطلاحاً «خود-اصالت‌سنج»[1] می‌باشند بدین معنا که نیاز به احراز هویت یا تأیید از سوی شخصی ندارند (علیدوستی شهرکی و دیگران، ۱۴۰۱: ۲۸۸).

درواقع، این نوع ادله به گونه‌ای طراحی شده اند که فناوری آن می‌تواند گواهی بر اصالت آن باشد. بعنوان مثال، برخی ادله‌ی دیجیتال رمزنگاری شده یا دارای «فراداده»[2]های

1. Self-authentication.
2. Metadata.

فراداده داده‌های مربوط به داده‌ها هستند و اصطلاحی است که برای توصیف اطلاعات مخفی مختلف ایجاد شده همراه با اسناد، عکس‌ها و فایل‌های رایانه، تلفن همراه یا سایر ابزارهای هوشمند استفاده می‌شود. فراداده معمولاً شامل تاریخ ایجاد فایل‌ها، زمان‌های ویرایش فایل اصلی، برچسب زمانی از آخرین ذخیره‌سازی و اطلاعات مربوط به کاربری که در ابتدا فایل را ایجاد کرده می‌شود. مشخص بودن فراداده‌های ادله‌ی دیجیتال به خصوص ادله‌ی ناشی از منابع باز، مانند برچسب‌های زمانی، آدرس آی‌پی و اطلاعات مرتبط با هویت شخص آپلودکننده‌ی اطلاعات به تأیید اصالت ادله بسیار کمک خواهد کرد.

ضمیمه شده یا اثر دیجیتال خاص یا همان «هش»[1]می‌باشند که می‌تواند اصالت آن ادله را اثبات کنند.

اما در برخی موارد این وضعیت صادق نخواهد بود و دیوان، سازمان‌های غیردولتی و کاربران اینترنت برای بدست آوردن فراداده‌های اطلاعات دیجیتال به سرورهای رسانه‌های اجتماعی دسترسی ندارند. در این خصوص در قضیه‌ی بمبا، دادستان اسکرین‌شات‌هایی از برخی عکس‌های آپلود شده در صفحات فیس‌بوک را بعنوان مدرک به دیوان ارائه داد. در پی این اقدام، وکیل متهم مسائل بسیاری را به چالش کشید؛ از جمله اینکه ادعا کرد با توجه به ویژگی‌های اسکرین‌شات، نمی‌توان اطلاعات مربوط به هویت فرد آپلودکننده را بدست آورد، زیرا برای ساخت یک حساب کاربری در فیس‌بوک نیازی به اطلاعات هویتی معتبر نیست و همچنین با توجه به روش دادستانی برای گردآوری اطلاعات و عدم دسترسی به سرورهای فیس‌بوک، برخلاف یک عکس واقعی، از یک اسکرین‌شات نمی‌توان فراداده‌های آن را بدست آورد (ICC-01/05-01/13, 2015: para. 83-85). البته شعبه‌ی رسیدگی‌کننده بدون ارائه‌ی دلیل، اسکرین‌شات‌ها را بعنوان مدرک پذیرفت.

با این حال، گردآوری اطلاعات از طرق روش مورد استفاده‌ی دادستان در قضیه‌ی بمبا، قابل نقد به نظر می‌رسد، زیرا همانطور که بیان شد برخلاف یک عکس اصیل و واقعی، فراداده‌های اسکرین‌شات همچون اطلاعات هویتی شخص آپلودکننده،

Silva, Jason, WHAT IS METADATA AND WHY IS IT CRITICAL TO A FORENSIC INVESTIGATION?, 27 Sep 2016, Last visited: 5 Jul 2024, at: https://cornerstonediscovery.com

1. Hash.

هشینگ یا هش، یک تکنیک دیجیتال است که برای اطمینان از صحت و سلامت داده‌ها استفاده می‌شود. در این فرایند، داده‌ها از طریق یک الگوریتم خاص پردازش می‌شوند تا یک کد منحصر به فرد به نام هش تولید شود. این کد شبیه به یک اثر انگشت دیجیتال است که به داده‌ها تعلق دارد و تغییرات در داده‌ها باعث تغییر هش می‌شود. بطور ساده، اگر حتی یک حرف یا عدد در داده‌های دیجیتال تغییر کند، هش آن بطور کامل متفاوت خواهد شد. این ویژگی بویژه در بررسی صحت اطلاعات در پرونده‌های کیفری و مستندسازی جرایم بسیار مفید است، زیرا کمک می‌کند تا اثبات شود که داده‌های دیجیتال پس از جمع‌آوری تغییر داده نشده اند.

Mossé Cyber Security Institute, "Digital Forensics: Hashing for Data Integrity", 2022, last visited: 5 January 2025, available at: Digital Forensics: Hashing for Data Integrity — MCSI Library.

برچسب‌های زمانی و محدوده‌ی جغرافیایی عکس گرفته‌شده مشخص نیست و همچنین دادستانی یا طرفین به سرورهای فیس‌بوک یا سایر شبکه‌های اجتماعی جهانی دسترسی ندارند تا بتوانند فراداده‌های مذکور را بدست آورند و فقدان چنین اطلاعاتی تأیید اصالت اسکرین‌شات و احراز هویت پدیدآورنده‌ی آن را با مشکل مواجه می‌کند. نکته‌ی دیگر اینکه فقدان امکانات برای دسترسی به فراداده‌های اسکرین‌شات، به نوعی متهم را در شرایط نابرابر با دادستان قرار داده و توان او برای به چالش کشیدن ادله‌ی دیجیتال مزبور را کاهش می‌دهد.

از سوی دیگر، برخی از ادله‌ی دیجیتال به دلیل پیچیدگی اطلاعات اولیه و نیاز به پردازش برای تبدیل به داده‌های قابل فهم نیازمند احراز اصالت یا هویت‌سنجی توسط کارشناسان می‌باشند (توحیدی و افضل‌پور، ۱۳۹۹: ۲۸۵)، بدین معنا که بعنوان مثال یک کارشناس فنی بایستی بتواند تأیید کند که ادله‌ی مزبور مورد تغییر و جعل قرار نگرفته است. در این راستا، استفاده از نیروهای خارجی مانند استفاده از ادله‌ی کارشناسی، یکی دیگر از اقدامات کاربردی برای تأیید و تقویت اصالت ادله‌ی دیجیتال می‌باشد. کارشناسان بواسطه‌ی مهارت و دانش تخصصی‌شان می‌توانند در مورد اصالت، منشأ و قابلیت اعتماد آن شهادت دهند. مثلاً در پرونده‌ی «الحسن»[1] دادستان دیوان از یک کارشناس فعال در حوزه‌ی تجزیه و تحلیل فیلم‌ها درخواست کرد که از ادله‌ی دیجیتال و پلتفرم‌هایی مانند «گوگل ارث»[2] برای مکان‌یابی بناهای تاریخی در منطقه‌ی تیمبوکتو مالی استفاده کند (Fan & Gillet, 2023: 668).

بنابر رویه‌ی قضایی دیوان و «رهنمودهای لایدن راجع به استفاده از ادله‌ی گرفته‌شده از منابع دیجیتال در دادگاه‌ها و دیوان‌های کیفری بین‌المللی»[3] که یک سند غیررسمی و غیرالزام‌آور برای دیوان محسوب می‌شود، مشخص بودن تاریخ و محل انتشار یک محتوای آنلاین یا مثلاً معین بودن آرم‌های منبع رسانه در ویدئوها نیز از نشانه‌های کافی برای احراز

1. Al Hassan.
2. Google Earth.
3. Leiden Guidelines on the Use of Digitally Derived Evidence in International Criminal Courts and Tribunals, 2021.

قابلیت اعتماد، اصالت منشأ و یکپارچگی ادله هستند (Aalto-Setälä, S. et al., 2021: 17). همچنین، مشخص بودن تاریخ انتشار ادله هم به احراز مؤلفه‌ی ارتباط و هم ارزش اثباتی ادله کمک بسیاری می‌کند. مثلاً در پرونده‌ی «انتاگاندا»[1] دادستان ده عکس را بعنوان مدرک دیجیتال به دیوان ارائه کرد که شعبه اظهار داشت شش عکس، تاریخ ندارند و به این علت نمی‌تواند مرتبط یا غیرمرتبط بودن آنها به پرونده و همچنین ارزش اثباتی آنها را تعیین کند. بعلاوه، دادستان در مورد تاریخ سه عکس از چهار عکس باقی‌مانده که دارای تاریخ بودند، اطلاعات بیشتری ارائه نکرده است و بنابراین نمی‌توان بطور قطع گفت که تاریخ آنها درست است یا خیر. شعبه، عکس چهارم را که مربوط به سال ۲۰۰۰ بود به علت آنکه تاریخ آن خارج از محدوده‌ی زمانی ارتکاب جرایم موضوع پرونده بود، مدنظر قرار نداد (ICC-01/04-02/06-1838, 2017: para. 68). در کل نظر شعبه این بود که بواسطه‌ی نبود اطلاعات مؤثق در مورد تاریخ، مکان و همچنین رویدادهای تصویر شده، ارزش اثباتی عکس‌ها به حدی پایین است که نمی‌توان آن‌ها را بعنوان ادله پذیرفت.

همانطور که اشاره شد، از دیگر عوامل دخیل در سنجش اصالت اولیه‌ی ادله‌ی دیجیتال، «زنجیره‌ی نگهداری» و «حفظ» ادله می‌باشد. زنجیره‌ی نگهداری نقش حیاتی در مستندسازی ادله ایفا می‌کند. مستندسازی ادله با هدف اثبات اصالت و حفظ وضعیت اولیه‌ی دلایل بدست‌آمده انجام می‌شود تا اطمینان حاصل شود که هیچ‌گونه تغییر یا تحریفی در آنها رخ نداده است. برای مثال، تصویری از یک گفت‌وگوی آنلاین می‌تواند بعنوان تأییدی بر وقوع مکالمه‌ی الکترونیکی مورد استناد قرار گیرد، به شرطی که ثابت شود بدون تغییر باقی مانده است (مؤذن‌زادگان و دیگران، ۱۳۹۴: ۷۹). شایان ذکر است که صرف جمع‌آوری ادله‌ی دیجیتال بدون مستندسازی کاری بیهوده تلقی می‌شود، زیرا برای حفظ ارزش اثباتی بایستی ادله با شیوه‌های خاص جمع‌آوری و نگهداری شوند (مؤذن‌زادگان و شایگان، ۱۳۸۸: ۹۷). در این راستا، زنجیره‌ی نگهداری در فرایند مستندسازی ادله‌ی دیجیتال این هدف مهم را در نظر دارد که اطمینان حاصل شود که

1. Ntaganda.

ادله‌ی دیجیتال ارائه شده، همان ادله‌ای هستند که در مبدأ، کشف شده و تا زمان استناد بدانها در دادگاه، دچار جعل یا تغییر نشده اند.

یکی از مواردی که موجب استحکام بیشتر زنجیره‌ی نگهداری می‌شود، مشخص بودن منشأ ادله‌ی دیجیتال (شاهد، نویسنده، هویت پدیدآورنده‌ی اطلاعات یا موارد دیگر) است. البته اثبات منشأ در حالتی که ممکن است مثلاً یک شخص هنگام ارسال پیام، از نام غیرواقعی استفاده کند، سخت خواهد شد که در این موارد بایستی سعی شود برای اثبات اصالت از آدرس آی‌پی و در صورت دسترسی، از سوابق اطلاعات دیجیتال نزد شرکت‌های ارائه‌دهنده‌ی خدمات استفاده کرد (السان و منوچهری، ۱۳۹۷: ۳۴). برخی مواقع نیز ممکن است منشأ ادله بصورت کلی قابل شناسایی نباشد که در این موارد، امکان دارد که ادله‌ی دیجیتال، «ادله‌ی شنیده‌ای ناشناس»[1]به شمار آیند. لازم به ذکر است که علی‌رغم اینکه منعی برای ارائه‌ی ادله‌ی شنیده‌ای در دیوان وجود ندارد و قابل پذیرش هستند، اما با توجه به رویه‌ی قضایی، دیوان برای ادله‌ی مذکور ارزش اثباتی کمی در نظر گرفته و بیشتر برای تأیید ادله‌ی دیگر از آن بهره برده است (ICC-01/04-01/06, 2007, paras. 101, 410).

البته برخی اوقات، دیوان برای پذیرفتن اطلاعات دیجیتال، یک زنجیره‌ی نگهداری کامل را لازم ندانسته است. در پرونده‌ی «لوبانگا»[2]وکلای متهم قابل اعتماد بودن برخی از ادله‌ی ارائه شده توسط دادستانی شامل تعدادی اسناد، گزیده‌های فیلم‌ها و همچنین ایمیل‌ها را با این ادعا که دادستان هیچ گونه اطلاعات دقیقی در رابطه با زنجیره‌ی نگهداری و انتقال آن‌ها ارائه نکرده و اینکه چنین مسئله‌ای اصالت ادله را مورد تردید قرار می‌دهد(ICC-01/04-01/06, 2007, para. 60)، به چالش کشیدند. آنها از شعبه خواستند که این ادله را نپذیرد یا ارزش اثباتی نسبتاً کمی برای آن‌ها قائل شود. در پاسخ، شعبه با رد این ادعا، اظهار می‌دارد که وکیل مدافع یک اعتراض کلی به قابل قبول بودن ادله مذکور داشته

1. Anonymous hearsay evidence.

ادله‌ی شنیده‌ای، ادله‌ای غیر مستقیم هستند که از منابعی غیر از نویسنده یا شخص اصلی که شاهد وقایع بوده اند، بدست آمده اند. مثلاً شاهد الف در دادگاه به حرفهایی که از شخص ب شنیده است، استناد می‌کند.

2. Lubanga.

است و در خصوص ادعای خویش، هیچ اشاره‌ای به یک مورد خاص نکرده و دلایل مورد توجهی نیز برای اثبات اعتراض خود ارائه نداده است. بعلاوه، اساسنامه یا آیین دادرسی و ادله‌ی دیوان در این خصوص که فقدان اطلاعات در مورد زنجیره‌ی نگهداری و انتقال، بر قابل قبول بودن یا ارزش اثباتی ادله‌ی دادستان اثر می‌گذارد، هیچ مقرره‌ی صریحی ندارند (ICC-01/04-01/06, 2007, paras. 96, 98)

لازم به ذکر است علی‌رغم اینکه ممکن است برای پذیرفته شدن داده‌ها و اطلاعات در دیوان، یک زنجیره‌ی نگهداری کامل لازم نباشد، اما یک زنجیره‌ی نگهداری دقیق و قوی، ارزش اثباتی ادله را افزایش می‌دهد که این امر موجب افزایش بار اثباتی اطلاعات نیز خواهد شد (Public International Law & Policy Group, 2022: 19). مشخص بودن منشأ ادله و نیز شهادت زنده نقش بسیاری در تأیید زنجیره‌ی نگهداری و به تبع آن افزایش بار اثباتی ادله‌ی دیجیتال دارد. از جمله اقداماتی که می‌توان جهت یافتن منشأ منابع دیجیتال مورد استفاده قرار داد، پیدا کردن اولین نسخه‌ی به اشتراک گذاشته شده و تلاش برای برقراری ارتباط با کسی است که اطلاعات را به اشتراک گذاشته است (Laving, 2014: 31).

در ارتباط با زنجیره‌ی نگهداری، اهمیت وظایف مستندسازان را نباید از نظر دور داشت، زیرا وظیفه‌ی آن‌ها جمع‌آوری، ذخیره و محافظت از ادله‌ی دیجیتال می‌باشد که به نوعی پاشنه‌ی آشیل زنجیره‌ی نگهداری به شمار می‌آید (جلالی‌فراهانی، ۱۳۸۶: ۱۰۳). راجع به این فرآیند برخی امور اهمیت بسیاری دارند؛ از جمله اینکه لازم است مستندسازان علاوه بر کوشش برای یافتن منشأ منبع یعنی هویت نویسنده‌ی مطالب و پدیدآورنده‌ی ادله‌ی دیجیتال، به فراداده‌ی ادله نیز توجه فراوانی داشته باشند، زیرا این امر می‌تواند اطلاعات دقیقی در باب زمان و مکان ثبت داده‌های ادله ارائه دهد (Public International Law & Policy Group, 2022: 16). همچنین، برای حفظ فراداده‌های اصلی ادله‌ی دیجیتال همانند ادله‌ی ویدئویی، تصویری و صوتی لازم است که از انتقال اطلاعات اصلی خودداری شود و دسترسی افراد غیرمتخصص به آن‌ها محدودتر شود. در غیر این صورت امکان دارد که مثلاً با انتقال یک عکس اصلی به دیگری در

«واتس‌اپ»[1] فراداده‌ی آن حذف شود (Public International Law & Policy Group, 2022: 17). بعلاوه، مستندسازان برای اطمینان از تغییر نیافتن اطلاعات دیجیتال می‌توانند از اقدامات احتیاطی و محافظتی همچون رمزگذاری، مستندسازی و تهیه‌ی نسخه‌های پشتیبان از اطلاعات استفاده کنند (محمدی و میری، ۱۳۸۸: ۱۶۱).

نکته‌ی آخر اینکه باید توجه داشت که ممکن است یک مدرک دارای اصالت تلقی شود، اما همچنان قابل اعتماد نباشد (ICC-01/05-01/08, 2016: para. 237)، لذا دیوان برای ارزیابی قابل اعتماد بودن ادله‌ی دیجیتال، در کنار اصالت، همه‌ی مؤلفه‌های قابل اعتماد بودن را با توجه به هر ادله در نظر خواهد گرفت.

۲-۱-۲. سایر شاخص‌های قابلیت اعتماد

دیوان در ارزیابی قابلیت اعتماد ادله‌ی دیجیتال، فقط به بررسی اصالت مدرک اکتفا نمی‌کند و «سایر شاخص‌های قابلیت اعتماد»[2]مهم و کلیدی همچون امکان سوءگیری منبع یک مدرک، ماهیت و ویژگی‌های خاص یک مدرک، همزمانی ثبت اطلاعات یک مدرک با اتفاق و ابزار مناسب برای ارزیابی ادله را نیز در نظر می‌گیرد.

راجع به شاخص اول، دیوان بررسی می‌کند که آیا منبع اطلاعات یک مدرک دیجیتال دارای سوءگیری نسبت به یکی از طرفین پرونده یا نتیجه‌ی پرونده است یا دارای استقلال و بی‌طرفی می‌باشد. در تشخیص این موضوع، دیوان به هدف ایجاد یک مدرک و همچنین انگیزه‌ی منبع اطلاعات توجه می‌کند. مثلاً ممکن است اطلاعات موجود در یک شبکه‌ی اجتماعی یا اخبار منتشر در یک روزنامه، به دلیل حمایت یک دولت خاص و اینکه آن شبکه و روزنامه به شدت تحت تأثیر دیدگاه‌های سیاسی دولت قرار دارد و منعکس‌کننده‌ی

---

1. WhatsApp.
2. Other criteria of reliability.

پرونده‌ی کاتانگا از جمله پرونده‌هایی است که ساختار منطقی‌تری را برای ارزیابی ارزش اثباتی ادله‌ی دیجیتال در نظر گرفته است. در این پرونده از دو مؤلفه‌ی قابلیت اعتماد (Reliability) و سایر نشانه‌های قابلیت اعتماد (Other criteria of reliability) برای ارزیابی ارزش اثباتی ادله‌ی مزبور نام برده شده است.

see ICC-01/04-01/07, TRIAL CHAMBER II, 17 December 2010, p. 19.

انگیزه‌های مغرضانه آن می‌باشد، بعنوان یک مدرک دیجیتال، قابل اعتماد دانسته نشود، زیرا چنین مسئله‌ای می‌تواند بر بی‌طرفی اطلاعات اثر منفی بگذارد. البته در صورتی که منبع و روش جمع‌آوری اطلاعات دیجیتال مشخص باشد، می‌تواند بعنوان نشانه‌ای از قابل اعتماد بودن ادله شناخته شود (Laving, 2014: 34). مثلاً شعبه‌ی محاکمه‌ی دیوان در قضیه‌ی «بمبا» در باب بی‌طرفی اشعار داشت که گزارش‌های سازمان‌های غیردولتی را می‌توان علی‌الظاهر قابل اعتماد دانست؛ مشروط بر اینکه تضمین‌های کافی برای بی‌طرفی ارائه دهد. در این باره، بررسی محتوای گزارش‌های مزبور نشان می‌دهد که گزارش‌ها اطلاعات رضایت‌بخشی در مورد منابع اطلاعاتی و روش‌شناسی خود ارائه کرده اند که اینها خود، نشانه‌های کافی از قابلیت اطمینان برای تضمین پذیرش آن‌ها می‌باشند (ICC-01/05-01/08, 2013, para. 21). همچنین ممکن است گروه‌های زیادی از افراد، از طرفداران متهم یا مظنون باشند و آن‌ها بر اساس انگیزه‌ای خاص، اطلاعات مغرضانه در رسانه‌های اجتماعی یا وبلاگ‌ها منتشر کنند که این امر نیز بر استقلال و بی طرفی ادله تأثیر می‌گذارد. در این راستا، اگرچه پی بردن به بی‌طرف بودن یا نبودن یک مدرک و همچنین انگیزه‌ی یک منبع یا اطلاعات ارائه شده ممکن است پیچیده باشد، اما به نظر می‌رسد بررسی مواردی چون تاریخچه‌ی رسانه، محتوای بارگذاری شده‌ی پیشین در صفحه‌ی اجتماعی مدنظر، زندگی‌نامه‌ی نویسنده و ارتباط آن با مظنون می‌تواند تا حد زیادی به پی بردن به مسئله کمک کند.

دیوان همچنین در بررسی ماهیت و ویژگی‌های خاص ادله‌ی دیجیتال بعنوان دیگر معیار قابلیت اعتماد، توجه می‌کند که این ادله توسط کاربر (مانند ویدئوها و عکس‌های تهیه شده از یک حادثه توسط شاهدان عینی) یا بصورت خودکار (مانند اطلاعات شخصی یا موقعیت زمانی و مکانی‌ای که یک برنامه‌ی تلفن همراه یا یک دستگاه و پلتفرم دیگر ثبت می‌کنند) ایجاد شده اند و منبع آنها بصورت بسته و خصوصی است یا باز و در دسترس عموم می‌باشند (ICC-01/04-01/07, 2010: para. 27). مثلاً در پرونده‌ی «کاتانگا»، شعبه در ارزیابی قابل اعتماد بودن ویدئوها و صوت‌های ضبط‌شده، به سراغ ماهیت و نحوه‌ی ایجاد اطلاعات ثبت شده در آنها بعنوان یکی از شاخص‌ها رفت. در کل به نظر

می‌رسد از آنجایی که ادله‌ی خودکار در مقایسه با ادله‌ی دیگر، کمتر در معرض خطای انسانی هستند، قابل اعتمادتر هستند.

همزمانی ثبت اطلاعات و داده‌های یک مدرک بعنوان دیگر شاخصه‌ی قابلیت اعتماد، بدین معناست که آیا اطلاعات و داده‌های در دست بررسی بلافاصله بعد از وقوع اتفاق تهیه شده اند یا با فاصله‌ی زمانی زیاد، اقدام به ثبت اتفاقات شده است. مثلاً اگر فیلمی حین وقوع جرمی یا بلافاصله بعد از آن ضبط شود، معیار مذکور را دارد. اما اگر همین ویدیو چند روز بعد از حادثه تهیه شود، همزمانی آن چالش‌برانگیز خواهد بود، چون ممکن است در همین فاصله، صحنه‌ی جرم تغییر داده شده باشد. در خصوص معیار همزمانی، برای نمونه در پرونده‌ی «بمبا»، هم دادستان و هم شعبه‌ی محاکمه از همزمانی صوت‌ها با اتفاقات بعنوان یکی از نشانه‌های قابل اعتماد بودن صوت‌ها و برخورداری آنها از ارزش اثباتی نام می‌برند (ICC-01/05-01/08-2299-Red, 2012: paras. 118-119, 123). در نمونه‌ای دیگر در پرونده‌ی «انتاگاندا»، شعبه اظهار داشت که ویدئوها و تصاویر ماهواره‌ای استناد شده در زمینه‌ی تخریب منطقه‌ی «لیپری»[1] توسط اتحادیه‌ی میهن‌پرستان کنگو و نیروهای میهن‌پرست برای آزادی کنگو، یک ماه بعد از حمله تهیه شده اند و بنابراین آن‌ها را در این پرونده، دارای کاربرد محدودی می‌داند. در عوض، شعبه ترجیح داد که به شواهد همزمان یعنی گزارش‌ها و مشاهدات شاهدان از جمله شاهدان عینی تکیه کند که در جریان حمله‌ی ۱۸ فوریه ۲۰۰۳ حضور داشتند یا بلافاصله بعد از آن به لیپری آمدند تا شاهد تخریب باشند (ICC-01/04-02/06, 2019: para. 569).

بعلاوه، دیوان در سنجش ابزار مناسب ارزیابی ادله بعنوان یکی دیگر از شاخصه‌های کلیدی قابل اعتماد بودن ادله‌ی دیجیتال، به بررسی امکان آزمایش و تأیید اطلاعات یک مدرک و روش جمع‌آوری آنها می‌پردازد (ICC-01/04-01/07, 2010: para. 27). طبیعتاً اگر اطلاعات و داده‌های ادله‌ی دیجیتال توسط اشخاص حرفه‌ای ثبت شوند و درباره‌ی صحت آن شهادت داده شود، قابل اعتمادتر تلقی می‌شوند. مثلاً در سال ۱۹۹۸ و در جریان رسیدگی به پرونده‌ی «جورج روتاگاندا»،[2] گوینده‌ی رادیو و معاون رئیس

1. Lipri.
2. George Rutaganda.

شبه‌نظامیان قوم «هوتو»، فیلم گرفته شده توسط «نیک هیوز» گزارشگر بریتانیایی و شهادت او، بعنوان یک مدرک مهم نقش اساسی در محکومیت این فرد ایفا کرد. البته ظاهراً این فیلم، حاوی چند پرش بود که بر اساس گزارش‌های واصله، دلیل این امر، آن بوده است که نیک هیوز، از نگرانی بابت تمام شدن باتری مجبور به توقف کار در چند نقطه شده است. با این حال، فیلم او توسط دادگاه تا حدی قابل اعتماد و دارای ارزش اثباتی شناخته شد، زیرا هم توسط یک خبرنگار حرفه‌ای که تجهیزات و بهترین نوع کیفیت فیلم در زمان و مکان مذکور را می‌شناخت، فیلم‌برداری شده بود و هم اینکه با توجه به موقعیت حرفه‌ای هیوز، زنجیره‌ی نگهداری فیلم قابل قبول بود (The Center for Research Libraries, 2012: 146) جالب اینکه شهادت «نیک هیوز» در خصوص فیلم، تأثیر مهمی در تقویت ارزش اثباتی فیلم داشت. این مسئله نشان می‌دهد که اگر ویدئوها با شهادت شاهد و سایر شواهد تأیید شوند، ممکن است قابل اعتمادتر تلقی شوند. البته لزومی ندارد هر کدام از ادله که به یک دادگاه یا دیوان ارائه می‌شوند از طریق شهادت شهود تأیید شوند، اما شعبه‌ی رسیدگی کننده باید متقاعد شود که مدرکی که ارائه شده شامل همان اطلاعاتی هست که مدرک به دنبال اثبات آن است که این مسئله یا در ظاهر مدرک مشهود است یا اینکه سایر ادله، قابل قبول بودن منشأ مدرک را نشان می‌دهند.

۲-۲. اهمیت ادله

دیگر مؤلفه‌ی مدنظر دیوان برای احراز ارزش اثباتی ادله‌ی دیجیتال، اهمیت ادله است. البته همانطور که اشاره شد مؤلفه‌ی اهمیت ادله، که در پرونده‌ی کاتانگا بصراحت مورد تأکید قرار گرفته، در برخی پرونده‌های دیگر مستقیماً ذکر نشده و غالباً از مؤلفه‌ی قابلیت اعتماد در رویه‌ی قضایی برای ارزیابی ادله‌ی دیجیتال استفاده شده است. از این رو، دلیل تمرکز بر چارچوب ارائه‌شده در پرونده‌ی کاتانگا، ساختار منطقی و منسجم آن در ارزیابی ارزش اثباتی ادله مستند است که از عناصر قابلیت اعتماد و اهمیت ادله بصورت هم‌زمان بهره می‌گیرد. بنابراین مؤلفه، ادله بایستی تا حد قابل توجهی بر تصمیمات دیوان اثر بگذارند تا پذیرفته شوند. تأثیرگذاری ادله بر تصمیم شعبه به دو طریق امکان‌پذیر است: الف) یک مدرک ممکن است بطرز قابل توجهی به شعبه جهت رسیدن به نتیجه در

خصوص وجود یا عدم وجود یک واقعیت در پرونده کمک کند. فرضاً یک عکس یا فیلم باید بتواند یکی از واقعیات موجود در پرونده، مثلاً دستور متهم به سربازان خود برای حمله به منطقه‌ای را نشان دهد. ب) یک مدرک ممکن است بطور قابل توجهی به شعبه به ارزیابی قابل اعتماد بودن سایر ادله موجود در پرونده کمک کند (ICC-01/04-01/07, Op. cit, para. 34).

شایان ذکر است که نباید مؤلفه‌ی اهمیت را با عنصر ارتباط آمیخت، زیرا ممکن است که یک مدرک دیجیتال مرحله‌ی اول یعنی ارتباط را برآورده کند، اما به اندازه‌ی کافی به شعبه برای متقاعد یا منصرف کردن او راجع به مسئله‌ای در پرونده کمک نکند. در این باره، دیوان تأثیر احتمالی پذیرش ادله بر پرونده را بررسی می‌کند و اگر تأثیر، تقریباً «کم رو به هیچ»[1]باشد، تقریباً بعید است که شعبه آن مدرک را بپذیرد، زیرا به تحقیقات کمکی نخواهد کرد. ولی اگر دامنه‌ی تأثیر پذیرش ادله از «حدودی تا قابل توجه»[2]باشد، احتمالاً به اندازه‌ی کافی مهم تلقی خواهند شد(ICC-01/04-01/07, Op. cit, para. 35).

۳. اثر جانبدارانه

سومین مرحله‌ی آزمون قابلیت پذیرش ادله، ارزیابی اثر جانبدارانه مدرک می‌باشد. اگرچه تعریف مشخص و دقیقی از اثر جانبدارانه‌ی ادله وجود ندارد، اما می‌توان گفت که این مرحله به تأثیر ارزش اثباتی ادله بر دادرسی منصفانه اشاره دارد؛ بدین معنا که اگر احراز شود که دلیل یا مدرکی بدون مبنا و توجیه قانونی، به نفع یک طرف پرونده می‌باشد، به نحوی که نقض جدی حق دادرسی منصفانه را به دنبال داشته باشد، می‌توان آن مدرک را دارای اثر جانبدارانه دانست. در این مرحله، دیوان ارزش اثباتی یک مدرک را در برابر اثر جانبدارانه‌ای که ممکن است ایجاد کند، می‌سنجد؛ بدین معنا که که ادله‌ی جانبدارانه بطور خودکار در روند ارزیابی ادله در دادگاه حذف نمی‌شوند، بلکه شعب تنها در صورتی تصمیم به حذف ادله می‌گیرند که اثر جانبدارانه‌ی احتمالی آنها از ارزش اثباتی ادله بیشتر باشد (Arcos Tejerizo, 2023: 762). در این خصوص، شعبه‌ی محاکمه در پرونده‌ی

1. Little to none.
2. Some to considerable.

«کاتانگا» اشعار داشته است، با اینکه امری عادی است که همه‌ی ادله‌ای که باعث متهم شناخته شدن فرد می‌شوند، جانبدارانه محسوب شوند، اما شعبه باید اطمینان حاصل کند که ادله علی‌رغم جانبدارانه بودن، غیرمنصفانه نیستند (ICC-01/04-01/07, 2010: para. 37). به عبارتی ادله‌ی دیجیتال جانبدارانه، ادله‌ای هستند که ممکن است باعث دادرسی غیرمنصفانه شوند (Freeman, 2021: 71). این مطلب نشان می‌دهد که جانبدارانه شناختن یک مدرک، لزوماً به معنای این نیست که آن مدرک حتماً ناقض دادرسی منصفانه است، بلکه این امر نیز باید توسط قضات احراز شود و در غیر این صورت، ادله، علی‌رغم جانبدارانه بودن پذیرفته می‌شوند. رویه‌ی قضایی دیوان نشان می‌دهد که قضات در اعمال بند ۴ ماده‌ی ۶۹ اساسنامه و تشخیص موضوع مذکور اختیار گسترده‌ای دارند و بسته به شرایط هر پرونده، تصمیم‌گیری می‌شود.

تعیین میزان اثر جانبدارانه‌ی یک مدرک باید بصورت موردی و با در نظر گرفتن ویژگی‌های خاص هر مدرک صورت گیرد. اثر جانبدارانه ممکن است به اشکال مختلفی بروز یابد که از آن جمله اند: ۱. نقض حق محاکمه‌ی متهم بدون تأخیر غیرموجه، ۲. نقض حق پرسش از شاهدان مخالف (حق پرسش متقابل) و ۳. نقض حق سکوت و کمک از وکیل طی بازجویی (ICC-01/04-01/07, 2010, paras. 40-55). بررسی‌ها نشان می‌دهد که در مرحله‌ی ارزیابی اثر جانبدارانه، ادله‌ی دیجیتال بیشتر با موارد ۱ و ۲ مواجه هستند و به عبارت دیگر، این دو، از چالش‌های جدی و مهم مرحله‌ی سوم محسوب می‌شوند که ممکن است نقض جدی حق بر دادرسی منصفانه را به دنبال داشته باشند.

محاکمه‌ی بدون تأخیر غیرموجه، بعنوان حق متهم در قسمت ج ماده‌ی ۶۷ (۱) اساسنامه‌ی رم آمده است. طبق این مقرره، اگر زمان پیش‌بینی‌شده برای ارائه‌ی یک مدرک خاص یا ارزیابی بعدی آن توسط شعبه با ارزش اثباتی بالقوه‌ی آن مدرک نامتناسب باشد و باعث تأخیر غیرموجه در محاکمه‌ی متهم شود، شعبه بایستی مدرک را کنار بگذارد. در واقع، متهم حق دارد که در فاصله‌ی زمانی مناسب محاکمه شود و نمی‌توان بدون دلیل موجه، تأخیر زیادی در محاکمه داشت (نجفی، ۱۳۹۸: ۴۴۴). هدف از اتخاذ چنین اقدامی جلوگیری از اتلاف وقت و تحمیل حجم زیاد مدارک و همچنین

ادله‌ی تکراری یا وقت‌گیر در دادرسی می‌باشد. به همین دلیل بود که مثلاً دادگاه کیفری بین‌المللی یوگسلاوی سابق به منظور سرعت بخشیدن به روند رسیدگی به پرونده‌ی «بلاسکیچ» تصمیم گرفت که شهادت برخی شهود را استماع نکند، زیرا از شهود به تعداد کافی در مورد همان موضوع قبلاً تحقیق شده بود و اینکه دست‌نوشته‌هایی از سایر محاکمات به عنوان ادله نیز در اختیار داشت (زاپالا، ۱۳۸۷: ۱۴۶). حال در مورد ادله‌ی دیجیتال باید گفت که بررسی ادله‌ی دیجیتال بویژه ادله‌ی دیجیتال ناشی از منبع باز به دلیل ماهیت فنی خاص این نوع ادله، معمولاً زمان‌بر و پیچیده است. این ادله باید به دقت مورد تحلیل و ارزیابی قرار گیرند تا اصالت و صحت آن‌ها تأیید شود. فرایند احراز هویت این ادله معمولاً نیازمند بررسی دقیق منابع، زمان و ابزارهای فنی ویژه است، زیرا ادله‌ی دیجیتال می‌توانند به راحتی تغییر کنند یا بصورت جعلی منتشر شوند. این پیچیدگی‌ها باعث می‌شود که تحلیل و ارزیابی این نوع ادله زمان بیشتری نسبت به ادله‌ی سنتی لازم داشته باشد. این تأخیر می‌تواند حق متهم برای محاکمه سریع و بدون تأخیر غیرموجه را نقض کند (Janfalk, Op. cit.: 91). بعلاوه کمبود آموزش و استانداردهای لازم برای جمع‌آوری و تحلیل ادله‌ی دیجیتال باعث تأخیر در کار کارشناسان بررسی ادله‌ی دیجیتال می‌شود، چراکه آن‌ها ممکن است به ابزارها و فناوری‌های مناسب دسترسی نداشته باشند. این تأخیرها می‌توانند حق متهم برای محاکمه بدون تأخیر غیرموجّه را تهدید کنند، زیرا روند رسیدگی به پرونده به خاطر مسائل فنی و عدم آمادگی کارشناسان طولانی‌تر می‌شود (Osco Escobedo Miguel, et al, 2023: 97). لذا دیوان بایستی در انتخاب ادله در مراحل ارتباط و ارزش اثباتی، دقت بالایی داشته باشد، تا با چنین مسئله‌ای روبرو نشود.

یکی دیگر از اشکال مهم اثر جانبدارانه، نقض حق پرسش متقابل است که مرتبط با اصل تساوی سلاح‌ها نیز می‌باشد. طبق این اصل، می‌بایست برابری و تعادل منصفانه‌ای میان فرصت‌های داده به طرفین برای ارائه‌ی دفاعیات وجود داشته باشد. البته برابری طرفین به این معنا نیست که متهم، وسایل و منابعی مشابه دادستان در اختیار داشته باشد، بلکه منظور آن است که طرفین برای ارائه‌ی مطالبشان وسایل و زمان در اختیار داشته باشند (فضائلی، ۱۳۸۷: ۳۳۵).

به چالش کشاندن ادله‌ی دیجیتال در یک مدت زمان محدود، در مواردی که حجم ادله زیاد است، برای طرف مقابل بسیار دشوار می‌باشد. بعلاوه، مشکل دسترسی در فناوری برای طرفین بویژه اقشار آسیب‌پذیرتر نیز وجود دارد، بدین صورت که ممکن است برخی از آنها به دلیل ناتوانی‌های جسمی یا شناختی نتوانند به درستی از ابزارهای دیجیتال یا محتوای پیچیده‌ی ادله‌ی دیجیتال استفاده کنند یا محتوای آن را به چالش بکشند که این مسئله مانع از آگاهی و مشارکت آنها در فرآیندهای قانونی می‌شود. بنابراین، لازم است فناوری‌ها و محتواها بطور خاص برای نیازهای متفاوت هر شخص طراحی شوند (office of the prosecutor policy on children, 2023: 36). همچنین با توجه به ماهیت پیچیده و تخصصی این ادله، امکان دارد طرفین بطور یکسان امکان بهره‌برداری و استفاده از ابزارهای فناوری و اطلاعات دیجیتال را نداشته باشند و این مسئله می‌تواند بر توانایی متهم برای درک و به چالش کشیدن ادله تأثیر منفی بگذارد. بعنوان مثال، در پرونده‌ی الفقی المهدی، متهم پس از اقرار به ارتکاب جرم، به دلیل هدایت عمدی برای تخریب میراث فرهنگی تحت عنوان عامل مشترک مجرم شناخته شد. در این خصوص، بسیاری اذعان داشتند که اقرار المهدی تا حد زیادی نتیجه‌ی ادله‌ی دیجیتال فراوانی بود که دیوان در اختیار داشت (Koenig et al, 2021: 2). مثلاً می‌توان به ویدئوهایی اشاره کرد که نشان می‌داد المهدی به تخریب میراث فرهنگی کمک می‌کند. حتی بازرسان نیز به این مطلب اشاره کردند که متهم و وکیل او هرگز فرصتی برای پرسش متقابل راجع به ادله‌ی دیجیتال ارائه‌ی شده علیه خود از جمله اطلاعات دیجیتال ناشی از منابع باز، گزارش‌های موقعیت جغرافیایی و پدیدآورندگان گزارش‌های پیدا نکردند و به این دلیل حق به چالش کشیدن ادله توسط متهم با مشکلاتی مواجه شده است (Koenig et al, 2021: 2). لذا نظر به آنچه گفته شد، بایستی اقداماتی اتخاذ شود که طرف مقابل نیز از روش گردآوری اطلاعات دیجیتال و منشأ منابع اطلاع یابد و فرصت کافی برای بررسی آن‌ها در اختیار داشته باشد، زیرا یکی از عناصر دادرسی منصفانه، حق داشتن فرصت کافی در دفاع است و متهم باید از زمان و تسهیلات کافی برای دفاع از خود برخوردار باشد (خداخواه، ۱۳۹۷:

۱۶۲)، در غیر این صورت، اصل تساوی سلاح‌ها رعایت نخواهد شد و امکان پرسش متقابل وجود نخواهد داشت.

این چالش‌ها و سایر چالش‌هایی که راجع به ملاحظات ارزش اثباتی گفته شد، ممکن است باعث شوند که یک مدرک صرفاً برخی از مؤلفه‌های ارزش اثباتی را برآورده کند و در نهایت دارای ارزش اثباتی کمی باشد که این مسئله می‌تواند منجر به بروز اثر جانبدارانه و دادرسی غیرمنصفانه شود. در این باره، برخی مواقع دیوان علی‌رغم ارزش اثباتی کم یک مدرک، به دلیل اثر جانبدارانه‌ی آن، از پذیرش آن خودداری کرده است. فرضاً ممکن است بازرسان در شبکه‌های اجتماعی با عکسی از متهم مواجه شوند که حکایت از رابطه‌ی دوستانه‌ی متهم با برخی از مظنونان پرونده داشته است. درست است که چنین اطلاعاتی می‌تواند به دیوان کمک بسیاری کند، اما اگر عکس کیفیت نامناسبی داشته باشد، به حدی که چهره‌ها در آن بصورت دقیق مشخص نباشند، ممکن است این امر باعث تردید در قابلیت اعتماد آن عکس و کاستن از ارزش اثباتی آن شود. چنین مسئله‌ای، اثر جانبدارانه را در پی دارد و می‌تواند به هنگام تصمیم‌گیری شعبه، باعث غلبه‌ی اثر جانبدارانه یک مدرک در برابر ارزش اثباتی آن و در نهایت رد آن مدرک شود. مثلاً در پرونده‌ی «انتاگاندا» شعبه از پذیرش یک گزارش ویدئویی که مدعی حضور یک کودک‌سرباز در «ایتوری» بود، بعنوان مدرک اجتناب کرد و بیان داشت که به جز اطلاعاتی که درمورد تاریخ پخش این گزارش وجود دارد، دادستان هیچ‌گونه مدرکی در مورد زمان فیلم‌برداری ارائه نکرده که این امر باعث کاهش ارزش اثباتی مدرک و غلبه‌ی اثر جانبدارانه شده است (ICC-01/04- 02/06-1838, 2017: para. 63).

همچنین در پرونده‌ی «بمبا»، دادستانی صوت ضبط شده‌ای را بعنوان مدرک ارائه داد که حاوی مصاحبه‌ی یک روزنامه‌نگار با متهم بود که در آن به خروج جنبش آزادی‌بخش کنگو از این کشور در مارس ۲۰۰۳ اشاره داشت (ICC-01/05-01/08-2299-Red, 2012: para. 121). شعبه معتقد بود این مدرک ارتباط حداقلی به تصمیم شعبه دارد و به دیوان کمکی نمی‌کند. همچنین اظهار داشت که این صوت، گزیده‌ای از یک مصاحبه‌ی طولانی‌تر است که دادستان فایل کامل آن و نیز اطلاعات مربوط به منبع، اصالت و صحت

آن را ارائه نکرده است. بر این اساس، شعبه ارزش اثباتی ادعایی صوت مزبور را باعث ایجاد اثر جانبدارانه‌ی بالقوه بر دادرسی منصفانه دانسته و آن را رد می‌کند (Ibid: paras. 121-122).

البته دیوان معمولاً در پرونده‌هایی که ادله‌ی دیجیتال به دلیل ارزش اثباتی پایین، بطور محدود و آن هم برای تأیید ادله‌ی دیگر مورد استفاده قرار گرفته اند، ادله را دارای اثر جانبدارانه ندانسته است. برای نمونه، شعبه‌ی محاکمه به هنگام ارزیابی برخی صوت‌های ضبط شده در پرونده‌ی فوق، با توجه به استفاده محدود از اطلاعات موجود در صوت‌ها، معتقد بود که هیچ دلیلی وجود ندارد که باور کند پذیرش آنها می‌توانند اثر جانبدارانه‌ای بر یک محاکمه‌ی عادلانه داشته باشد و بنابراین بعنوان یک مدرک قابل پذیرش می‌باشند (Ibid: para. 123-124).

بعنوان مطلب پایانی این قسمت، دلیل اهمیت ویژه‌ی مرحله‌ی سوم این است که حتی اگر یک مدرک دیجیتال دارای ارزش اثباتی باشد، اما با سوءگیری، به اصول دادرسی منصفانه از جمله حقوق متهم به گونه‌ای جدی آسیب بزند که ضرر ناشی از پذیرش آن، بیشتر از ارزش اثباتی ادله در اثبات یک موضوع باشد، ممکن است دیوان علی‌رغم وجود ارزش اثباتی، دلیل را نپذیرد که این مسئله بیشتر در ادله‌ی دیجیتال دارای ارزش اثباتی پایین دیده می‌شود.

نتیجه

فرایند پذیرش ادله‌ی دیجیتال در دیوان کیفری بین‌المللی شامل مراحل ارتباط، ارزش اثباتی و اثر جانبدارانه می‌باشد که به نظر می‌رسد نمی‌توان مابین این مراحل، به لحاظ اهمیت قائل به اولویت‌بندی شد. در مرحله‌ی ارتباط، دیوان آستانه‌ی پایینی برای مرتبط قلمداد کردن ادله بصورت علی‌الظاهر در نظر می‌گیرد. اگرچه این رویکرد زمان‌بر می‌باشد، اما از آنجایی که رسیدگی به جنایات بین‌المللی با توجه به ماهیت جدی و گسترده‌ی آنها، ادله‌ی بیشتر و زمان طولانی‌تری برای بررسی را می‌طلبد، بنابراین لحاظ آستانه‌ی پایین برای مرتبط قلمداد کردن ادله منطقی به نظر می‌رسد؛ با این دقت نظر که دیوان در زمان بررسی مؤلفه‌ی اهمیت ادله در مرحله‌ی ارزش اثباتی، ادله‌ی با اهمیت کمتر

را یا نادیده بگیرد یا از آن‌ها جهت شفاف‌سازی سایر واقعیات موجود در پرونده استفاده کند.

دیوان در ارزیابی ارزش اثباتی ادله‌ی دیجیتال بعنوان مرحله‌ی دوم، به شاخصه‌های قابلیت اعتماد و اهمیت ادله برای پرونده توجه می‌کند. اگرچه مؤلفه‌ی قابلیت اعتماد، شاخص‌های متعددی را شامل می‌شود، اما رویه‌ی قضایی دیوان نشان می‌دهد که موضوعات یکپارچگی، مشخص بودن یا نبودن زمان و محل ثبت اطلاعات، منشأ ادله، زنجیره‌ی نگهداری و نحوه‌ی حفظ ادله، انگیزه‌ی منبع، همزمانی ثبت اطلاعات و داده‌ها با وقایع، روش جمع آوری ادله و امکان تأیید و پرسش از آنها، مهمترین شاخص‌های مدنظر دیوان هستند. درخور توجه است که دیوان برای تعیین بار اثباتی ادله، به میزان برآورده شدن مؤلفه‌های ارزش اثباتی بصورت یک کل توسط ادله‌ی دیجیتال توجه ویژه‌ای دارد و هرچه این مؤلفه‌ها، بیشتر برآورده شوند، میزان بار اثباتی آن در قضاوت نهایی افزایش خواهد یافت. این در حالی است که گاه تأمین مؤلفه‌های ارزش اثباتی دشوار می‌شود؛ از این جهت که ادله‌ی دیجیتال غالباً در معرض چالش‌هایی همچون جعل و تغییر اطلاعات، مشخص نبودن منشأ و انگیزه‌ی منبع و زمان و محل ثبت اطلاعات قرار دارند که عدم آشنایی قضات با آنها، می‌تواند موجب شود که ادله‌ی دیجیتالِ مخرب و آسیب‌زننده به حق بر دادرسی عادلانه، بار اثباتی قابل توجهی پیدا کنند. به تبع، چنین وضعیتی، طرفین پرونده را از لحاظ امکانات دفاع در وضعیت نابرابری قرار داده و حق بر پرسش متقابل را نقض خواهد کرد.

بررسی اثر جانبدارانه‌ی ادله در برابر ارزش اثباتی، مرحله‌ی نهایی پذیرش ادله‌ی دیجیتال در دیوان می‌باشد. با توجه به قواعد و رویه‌ی قضایی دیوان، به نظر می‌رسد این نهاد آستانه‌ی بالایی در زمینه‌ی اثر جانبدارانه‌ی ادله‌ی دیجیتال بر دادرسی منصفانه مدنظر دارد و صرفاً زمانی که ارزش اثباتی یک مدرک به گونه‌ای باشد که باعث اثر جانبدارانه‌ی جدی شود، آن مدرک را رد می‌کند. در واقع، هر چقدر که ادله بصورت دقیق‌تری ملاحظات و مؤلفه‌های ارزش اثباتی را برآورده کنند، کمتر در معرض اثر جانبدارانه قرار خواهند داشت. نهایتاً قضات دیوان در صورتی که با توجه به اطلاعات بدست آمده،

مدرکی را بصورت یک کل، واجد شرایط مراحل سه‌گانه‌ی پذیرش ادله بدانند و مطابقت آنها با سایر اطلاعات و ادله‌ی موجود در پرونده احراز کنند، در رأی خود بار اثباتی قابل توجهی برای آن در نظر خواهند گرفت، در غیر این صورت یا ادله رد می‌شوند یا در صورت کم بودن بار اثباتی آنها، جهت تأیید دیگر مدارک پرونده استفاده می‌شوند.

دیگر یافته‌ی مهم این مقاله این است که رویکرد منعطفانه‌ی فعلی دیوان در آزمون و پذیرش ادله‌ی دیجیتال، سودمند اما کافی نیست و این نهاد برای استفاده‌ی هر چه تمام‌تر از ظرفیت‌های چنین ادله‌ای، نیاز به یک رویکرد ساختارمندانه نیز دارد. دیوان فاقد دستورالعمل رسمی و الزام‌آور در خصوص ارزیابی ادله‌ی دیجیتال می‌باشد و تمرکز صرف بر رویه‌ی قضایی گذشته، نمی‌تواند به اندازه‌ی کافی چالش‌های آزمون ادله‌ی دیجیتال در دادرسی‌های آینده را رفع کند. لذا برای ایجاد تعادل بین پذیرش ادله و حقوق طرفین پرونده، ضرورت دارد که علاوه بر تنظیم یک دستورالعمل رسمی، استفاده از کارشناسان آشنا به مسائل فنی ادله‌ی دیجیتال و افزایش دانش قضات در باب چالش‌های فنی ادله، دیوان زمان و امکانات فنی لازم همچون کارشناسان خبره و معتمد برای پرسش متقابل از ادله‌ی مذکور را در اختیار متهم و وکلای مدافع او نیز قرار دهد. این کار موجب می‌شود تا از یک طرف، اگر ادله‌ای دارای ارزش اثباتی هستند، دیوان با در نظر گرفتن بار اثباتی قابل توجه برای آنها، در جهت مقابله‌ی جدی‌تر با بی‌کیفرمانی متهمان و احقاق حق قربانیان قدم بردارد و از طرف دیگر، حقوق متهم برای یک دادرسی منصفانه از جمله حق پرسش متقابل و محاکمه بدون تأخیر غیرموجه، در نتیجه‌ی استفاده از ادله‌ی دارای ارزش اثباتی کم، بطور جدی نقض نشود. همچنین نیاز است که دیوان همکاری خود با بازیگران خصوصی همچون شبکه‌های اجتماعی آنلاین را به منظور حفظ ادله‌ی دیجیتال ارزشمند و امکان بررسی فراداده‌ها البته با در نظر گرفتن تدابیر سختگیرانه برای اطمینان از مورد تهدید و آسیب قرار نگرفتن کاربران افزایش دهد.

تعارض منافع

تعارض منافع وجود ندارد.

ORCID

Ziba Nilaei Sangari https://orcid.org/0009-0004-3286-7394

Aghil Mohammadi https://orcid.org/0000-0002-7994-1641

منابع

توحیدی، احمدرضا، افضل‌پور، فاطمه. (۱۳۹۹)، «تحلیلی بر نحوه‌ی ارائه‌ی ادله و استنادپذیری داده‌های سنجش از راه دور در محاکم بین‌المللی»، فصلنامه‌ی تحقیقات حقوقی، شماره‌ی ۹۰. https://doi.org/10.29252/lawresearch.23.90.263

جلالی‌فراهانی، امیرحسین. (۱۳۸۶). «استنادپذیری ادله‌ی الکترونیکی در امور کیفری»، حقوق اسلامی، شماره‌ی ۱۵.

حیدری، مهدی. (۱۴۰۰). «حدود و ثغور ارزش اثباتی ادله الکترونیکی در حقوق کیفری»، همایش علمی مطالعات حقوقی، علوم قضایی و پژوهش‌های اجتماعی.

خداخواه، نسیم. (۱۳۹۷). «حقوق بزهدیده و متهم در دیوان کیفری بین‌المللی»، وکیل مدافع، دوره‌ی ۸، شماره‌ی ۱۷.

داودی بیرق، حسین (۱۳۸۷). ادله اثبات دعاوی حقوقی در فضای سایبر و مجازی، پایان‌نامه‌ی کارشناسی ارشد حقوق خصوصی، دانشکده‌ی حقوق و علوم سیاسی دانشگاه شیراز.

روح‌بخش، فرزاد (۱۴۰۲). اسناد الکترونیک در دادرسی مدنی، پایان‌نامه‌ی کارشناسی ارشد حقوق خصوصی، دانشکده‌ی حقوق و علوم سیاسی دانشگاه شیراز.

زاپالا، سالواتور. (۱۳۸۷). *حقوق بشر در محاکمات کیفری بین‌المللی*، ترجمه‌ی حسین آقائی جنت مکان، چ ۱، اهواز، دانشگاه شهید چمران اهواز.

السان، مصطفی، منوچهری، محمدرضا. (۱۳۹۷). «ارزیابی اصالت ادله‌ی الکترونیکی و ارزش اثباتی آن‌ها»، مطالعات حقوقی، دوره‌ی ۲، شماره‌ی ۱۰. https://doi.org/10.22099/jls.2018.28058.2765

علیدوستی شهرکی، ناصر، کشاورز، علی و صادقی اصل، علیرضا. (۱۴۰۱)، «قاعده‌گزینی جهت پذیرش ادله‌ی الکترونیک در نظام حقوقی ایران و آمریکا»، مجله‌ی حقوقی دادگستری، دوره‌ی ۸۶ شماره‌ی ۱۱۹. https://doi.org/10.22106/jlj.2021.530190.4171

فضائلی، مصطفی. (۱۳۸۷). *دادرسی عادلانه: محاکمات کیفری بین‌المللی*، چ ۱، تهران، مؤسسه‌ی مطالعات و پژوهشهای حقوقی شهردانش.

فیضی چکاب، غلام نبی، «اعتبار حقوقی دلیل و امضای الکترونیکی (مرور اجمالی برخی منابع ملی و بین‌المللی)». (۱۳۸۹)، پژوهش حقوق و سیاست، سال دوازدهم، شماره‌ی ۳۰.

مؤذن‌زادگان، حسنعلی، سلیمان دهکردی، الهام و یوشی، مهشید. (۱۳۹۴)، «حفظ صحت و استنادپذیری ادله‌ی الکترونیک با استفاده از بیومتریک و رمزنگاری»، پژوهش حقوق کیفری، سال چهارم، شماره‌ی دوازدهم.https://doi.org/10.22054/jclr.2015.1782

مؤذن‌زادگان، حسنعلی، شایگان، محمدرسول. (۱۳۸۸)، «استنادپذیری و تحصیل ادله‌ی الکترونیکی در حقوق کیفری ایران»، فصلنامه‌ی دیدگاه‌های حقوقی، شماره‌ی ۴۸.

محمدی، سام، میری، حمید. (۱۳۸۸). «بررسی تطبیقی ارائه‌ی ادله‌ی الکترونیک در دادگاه؛ اشکال و اعتبار آن»، فصلنامه‌ی علمی حقوق تطبیقی دانشگاه مفید، شماره‌ی ۱۷.

نجفی، سینا. (۱۳۹۸). «واکاوی معایب و مزایای سیستم رسیدگی و تعیین مجازات در دیوان کیفری بین‌المللی»، فصلنامه‌ی بین‌المللی قانون‌یار، دوره‌ی ۱۱، شماره‌ی ۳.

References

"Trial of the Major War Criminals Before the International Military Tribunal, Nuremberg: International Military Tribunal", vol. Xlll, Nuremberg, Germany, 1947.

Aalto-Setälä, S. et al. (2021). Leiden Guidelines on the Use of Digitally Derived Evidence in International Criminal Courts and Tribunals.

Arcos Tejerizo, M. (2023). "Digital evidence and fair trial rights at the International Criminal Court". Leiden Journal of International Law, No. 36. https://doi.org/10.1017/S0922156523000031

Ashouri, A., Bowers, C., Warden, C. (2014). "An Overview of the Use of Digital Evidence in International Criminal Courts", The 2013 Salzburg Workshop on Cyber Investigations, Vol.11. https://doi.org/10.14296/deeslr.v11i0.2130

Avveduto, S., Conti, S., Luzi, L., Pisacane, L., (2018). The Conceptual Representation of the "Electronic Evidence" Domain; Handling and Exchanging Electronic Evidence Across Europe, Vol.39, Switzerland, Springer.

Braga da Silva, R., (2021). "Updating the Authentication of Digital Evidence in the International Criminal Court", International Criminal Law Review, Vol. 22, No.5-6. https://doi.org/10.1163/15718123-bja10083

Freeman, L., (2019). "Prosecuting Atrocity Crimes with Open Source Evidence: Lessons from the International Criminal Court", in: Digital Witness Using Open Source Information for Human Rights Investigation, Documentation, and Accountability, Oxford: Oxford University Press.

Freeman, L., (2021). "Hacked and Leaked: Legal Issues Arising From the Use of Unlawfully Obtained Digital Evidence in International Criminal Cases", UCLA Journal of International Law and Foreign Affairs, Vol. 25, No.2.

Freeman, L., Vazquez Llorente, R., (2021). "Finding the Signal in the Noise: Finding the Signal in the Noise: International Criminal Evidence and Procedure in the Digital Age", Journal of International Criminal Justice, Vol. 19, Issue. 1. https://doi.org/10.1093/jicj/mqab023

Gillet, M., Fan, W. (2023). "Expert Evidence and Digital Open Source Information: Bringing Online Evidence to the Courtroom", Journal of International Criminal Justice, Vol. 21, Issue 4. https://doi.org/10.1093/jicj/mqad050

Hellwig, K., (2022). "The Potential and the Challenges of Digital Evidence in International Criminal Proceedings", International Criminal Law Review, Vol. 22, No. 5-6. https://doi.org/10.1163/15718123-bja10110

Human Rights Center UC Berkeley (2014). Digital Fingerprints: Using Electronic Evidence to Advance Prosecutions at the International Criminal Court.

ICC-01/04-01/06, PRE-TRIAL CHAMBER I, 29 January 2007.

ICC-01/04-01/07, TRIAL CHAMBER II, 17 December 2010.

ICC-01/04-02/06-1838, TRIAL CHAMBER VI, 28 March 2017.

ICC-01/04-02/06, TRIAL CHAMBER VI, 8 July 2019.

ICC-01/05-01/08-2299-Red, TRIAL CHAMBER III, 08 October 2012.

ICC-01/05-01/08, TRIAL CHAMBER III, 21 March 2016.

ICC-01/05-01/08, TRIAL CHAMBER III, 27 June 2013.

ICC-01/05-01/13, TRIAL CHAMBER VII, 9 October 2015.

ICTR-98-44-T, Trial Chamber III, 25 January 2008.

IT-05-88/2-T, Prosecutor v Tolimir (Judgement), Trial Chamber II, 12 December 2012.

Janfalk, D., (2021). Fact-Finding Online – A Fair Trial Offline? An Analysis of the Admissibility of Digital Open-Source Evidence in Relation to Trial Fairness at the International Criminal Court, Master's thesis, faculty of law, Lund University.

Kayyali, D., Althaibani, R., Ng, Y. (2021). "Digital Video Evidence, When Collected, Verified, Stored, and Deployed Properly, Presents New Opportunities for Justice", Last visited: July 23, 2024, at: https://iccforum.com/cyber-evidence

Koenig, A., Irving, E., McDermott, Y., Murray, D., (2021). "New Technologies and the Investigation of International Crimes: An Introduction", Journal of International Criminal Justice, Vol. 19, Issue 1. https://doi.org/10.1093/jicj/mqab040

Lane, A. (2021). "Atrocities on Camera: Solutions to Admissibility Issues with Digital Evidence at the International Criminal Court", Last visited: July 20, 2024, at: https://bytes.scl.org/untitled/

Laving, L., (2014). The Reliability of Open Source Evidence In the International Criminal Court, Master Thesis, International Human Rights Law, Lund University.

Mimran, T., Weinstein, L. (2023), "DIGITALIZE IT: DIGITAL EVIDENCE AT THE ICC", Last visited: July 2, 2024, at: https://lieber.westpoint.edu/digitalize-it-digital-evidence-icc/

Mossé Cyber Security Institute, "Digital Forensics: Hashing for Data Integrity", 2022, last visited: 5 January 2025, available at: Digital Forensics: Hashing for Data Integrity — MCSI Library

Niezen, R. (2023). "International Criminal Court is using digital evidence to investigate Putin – but how can it tell if a video or photo is real or fake?", Last visited: July 20, 2024 at: https://theconversation.com

Osco Escobedo Miguel, A., et al. (2023). "digital evidence as a means of proof in criminal proceedings", russian law journal, Volume XI, Issue 5. https://dx.doi.org/10.52783/rlj.v11i5s.895

OTP (2023). OFFICE OF THE PROSECUTOR POLICY ON CHILDREN.

Prosecutor v. Zlatko Aleksovski, DECISION ON PROSECUTOR'S APPEAL ON ADMISSIBILITY OF EVIDENCE, ICTY, Appeals Chamber, 16 February 1999.

Public International Law & Policy Group (2022). Chain of Custody In International Courts Training For Civil Society Documenters,

Quilling, Ch. (2022). "The Future of Digital Evidence Authentication at the International Criminal Court, Journal of Public & International Affairs", Online at: https://jpia.princeton.edu

Ragni, Ch. (2023). Digital evidence in international criminal proceedings and human rights challenges, EU and comparative law issues and challenges series (ECLIC), Vol. 7. https://doi.org/10.25234/eclic/28255

Rome Statute of the International Criminal Court, 17 July 1998.

Roscini, M., (2016). "Digital Evidence as a Means of Proof before the International Court of Justice", Journal of Conflict and Security Law, Vol. 21, Issue. 3. https://doi.org/10.1093/jcsl/krw016

SCSL-03-01-T-745, PROSECUTOR v. Charles Ghankay TAYLOR, TRIAL CHAMBER II, 25 February 2009.

Silva, Jason, WHAT IS METADATA AND WHY IS IT CRITICAL TO A FORENSIC INVESTIGATION?, 27 Sep 2016, Last visited: 5 Jul 2024, at: https://cornerstonediscovery.com

Stavrou, K. (2021). "Open-Source Digital Evidence in International Criminal Cases: A Way Forward in Ensuring Accountability for Core Crimes?", Last visited: August 3, 2024, at: https://opiniojuris.org/2021/01/26/

STL-11-01/T/TC, Prosecutor v Ayyash et al (Decision on the Prosecution Motions for the Admission of the Call Sequence Tables Related to the Five Colour-Coded Mobile Telephone Groups and Networks), Trial Chamber, 31 October 2016.

The Center for Research Libraries (2012). Human Rights Electronic Evidence Study.

The International Bar Association (2016). Evidence Matters in ICC Trials", 2016.

Translated References into English

Alidousti Shahraki, Naser; Keshavarz, Ali; Sadeghi Asl, Alireza. "Rule-Making for the Acceptance of Electronic Evidence in the Legal Systems of Iran and the United States," Justice Law Journal, vol. 86, no. 119, 2022, https://doi.org/10.22106/jlj.2021.530190.4171. [In Persia]

Davoudi Bairagh, Hossein. Evidence in Civil Litigation in Cyber and Virtual Space, Master's Thesis in Private Law, Faculty of Law and Political Science, Shiraz University, 2008. [In Persia]

Elsan, Mostafa; Manouchehri, Mohammadreza. "Evaluation of the Authenticity and Evidentiary Value of Electronic Evidence," Legal

Studies, vol. 2, no. 10, 2018, https://doi.org/10.22099/jls.2018.28058.2765. [In Persia]

Fazaeli, Mostafa. Fair Trial: International Criminal Proceedings, 1st ed., Tehran: Shahr-e-Danesh Institute for Legal Studies and Research, 2008. [In Persia]

Feyzi Chakab, Gholam Nabi. "The Legal Validity of Evidence and Electronic Signatures (A Brief Review of Some National and International Sources)," Law and Politics Research, vol. 12, no. 30, 2010. [In Persia]

Heidari, Mehdi. "The Limits and Scope of the Evidentiary Value of Electronic Evidence in Criminal Law," Scientific Conference on Legal Studies, Judicial Sciences, and Social Research, 2021. [In Persia]

Jalali-Farahani, Amirhossein. "The Admissibility of Electronic Evidence in Criminal Matters," Islamic Law, no. 15, 2007. [In Persia]

Khodakhah, Nasim. "The Rights of Victims and Defendants in the International Criminal Court," Vakilmodafe, vol. 8, no. 17, 2018. In Persia]

Moazenzadegan, Hossein-Ali; Shayegan, Mohammad Resoul. "The Admissibility and Collection of Electronic Evidence in Iranian Criminal Law," Legal Perspectives Quarterly, no. 48, 2009. [In Persia]

Moazenzadegan, Hossein-Ali; Soleiman Dehkordi, Elham; Youshi, Mahshid. "Ensuring Integrity and Admissibility of Electronic Evidence Using Biometrics and Encryption," Criminal Law Research, vol. 4, no. 12, 2015, https://doi.org/10.22054/jclr.2015.1782. [In Persia]

Mohammadi, Sam; Miri, Hamid. "A Comparative Study of the Presentation of Electronic Evidence in Courts: Forms and Validity," Comparative Law Scientific Quarterly, Mofid University, no. 17, 2009. [In Persia]

Najafi, Sina. "An Analysis of the Advantages and Disadvantages of the Trial and Sentencing System in the International Criminal Court," International ghanoonyar Quarterly, vol. 11, no. 3, 2019. [In Persia]

Rouhbakhsh, Farzad. Electronic Documents in Civil Procedure, Master's Thesis in Private Law, Faculty of Law and Political Science, Shiraz University, 2023. [In Persia]

Tohidi, Ahmadreza; Afsalpour, Fatemeh. "An Analysis of the Presentation and Admissibility of Remote Sensing Data in International Courts," Legal Research Quarterly, no. 90, 2020, https://doi.org/10.29252/lawresearch.23.90.263. [In Persia]

Zappalà, Salvatore. Human Rights in International Criminal Trials, trans. Hossein Aghaei Jannat Makan, 1st ed., Ahvaz: Shahid Chamran University of Ahvaz, 2008. [In Persia]

استناد به این مقاله: نیلائی سنگری, زیبا و محمدی, عقیل . (۱۴۰۴). قابلیت پذیرش ادله‌ی دیجیتال در دیوان بین‌المللی کیفری. *پژوهش حقوق کیفری*، (۴۸) ۱۳، ۴۱-۸۴.

Doi: 10.22054/jclr.2025.81549.2697