

The ICC enters into the future: the digital-evidence revolution or evolution?¹

O TPI ingressa no futuro: a revolução ou evolução das provas digitais?

Hanna Kuczyńska²

Institute of Law Studies of the Polish Academy of Sciences, Warsaw, Poland

hkuczynska@gmail.com

 <https://orcid.org/0000-0002-1446-2244>

ABSTRACT: Investigations into core international crimes should take into consideration the new, digital environment of evidence gathering. They cannot be conducted based solely on analogue means in a world that has become digital so fast. The ICC is taking an active part in the digital revolution in its investigations of core crimes, by establishing a new model of coping with the gathering, analysis, and management of digital evidence: the OTPLink and Project Harmony. In this article, firstly the response of the Office of the Prosecutor (OTP) to the digital environment of evidence-gathering is analyzed, whereby the OTP decided to use algorithms in order to more effectively manage evidence. The legal character of these new developments is analyzed, as well as the dangers they pose for the assessment of evidence and the fact-finding process. In this analysis it is also necessary to establish whether this is indeed a “AI revolution”. Further analysis will focus on answering the question whether the digitalized tools used by the OTP fulfill all the preconditions necessary in order to ensure the credibility and authenticity of digital evidence. At the same time it is necessary to distinguish between the

¹ Funding for the research: The research project was financed from the funds of the National Centre of Science (Narodowe Centrum Nauki) granted on the basis of a contract No. UMO-2023/49/B/HS5/02623 for a project entitled “In search of justice for core crimes in the digital age.”

² Dr hab., professor at the Institute of Law Studies of the Polish Academy of Sciences in Warsaw, Criminal Law Department.

case law of the Chambers that relies on the traditional assessment of open sources, and the Internet-derived evidence based on the revolutionized algorithm-based gathering and management of evidence by the OTP. To this end there is a need to analyze the attitude toward digital evidence adopted so far by the Chambers with respect to the assessment of digital evidence and the use of such evidence in fact-finding. The key question that needs to be answered is whether the revolution is taking place only before the OTP, whereas the Chambers adopt a more evolutionary attitude.

KEYWORDS: the international criminal court; project harmony; digital evidence; rules governing the admissibility of evidence.

RESUMO: *As investigações sobre crimes internacionais graves devem levar em consideração o novo ambiente digital de coleta de provas. Não é possível conduzi-las baseando-se exclusivamente em meios analógicos em um mundo que se tornou digital tão rapidamente. O Tribunal Penal Internacional (TPI) participa ativamente da revolução digital na investigação de crimes graves, estabelecendo um novo modelo para lidar com a coleta, análise e gestão de provas digitais: o OTPLink e o Projeto Harmony. Neste artigo, primeiramente, será analisada a resposta do Gabinete do Procurador (OTP) ao ambiente digital de coleta de provas, onde o OTP decidiu utilizar algoritmos para gerenciar provas de forma eficaz. O caráter jurídico desses novos desenvolvimentos será analisado, bem como os perigos que eles apresentam para a avaliação de provas e o processo de apuração dos fatos. Nesta parte, será também necessário estabelecer se isso constitui, de fato, uma "revolução da IA". Além disso, a análise abordará a questão de saber se as ferramentas digitalizadas utilizadas pelo OTP cumprem todos os pré-requisitos no que diz respeito à credibilidade e autenticidade das provas digitais. Contudo, é necessário distinguir entre a jurisprudência das Câmaras, que se baseia na avaliação tradicional de fontes abertas e provas derivadas da internet, e a coleta e gestão de provas baseada em algoritmos revolucionados pelo OTP. Para esse fim, é preciso analisar a atitude adotada até o momento pelas Câmaras em relação à avaliação das provas digitais e ao uso dessas provas na apuração dos fatos. A questão central que precisa ser respondida é se a revolução está ocorrendo apenas no âmbito do OTP, enquanto as Câmaras apresentam uma atitude mais evolutiva.*

PALAVRAS-CHAVE: *tribunal penal internacional; projeto harmonia; provas digitais; regras de admissibilidade probatória.*

1. INTRODUCTION

The character and scale of core international crimes³ not only require special forms of gathering evidence, but also must take into account the usage of these forms: it would take years to watch the relevant video evidence and read all the information available in the Internet in open sources. Such qualities (digital) and quantities (abundance of evidence) in an investigation is a 21st Century phenomenon and requires a new attitude when it comes to types of admissible evidence, their verification, management, and rules of their admissibility. The unique environment of evidence gathering requires a new approach – and technology is the key to this approach. Investigation into core crimes cannot be conducted based solely on analogue means in a world that has become so rapidly digital. The International Criminal Court takes an active part in the digital revolution in its investigations into core crimes. The recent developments with respect to harnessing technology in the task of gathering and managing evidence introduced before the ICC has become an important part of the search for justice vis-à-vis core crimes in the digital age.

The ICC is functioning in an environment where today hundreds of thousands of pieces of digital evidence and footages of violations of international humanitarian law (IHL) and violations of international human rights (IHR) are downloaded by potential witnesses⁴. Digital evidence acquired from open sources (OSINT) has become a new and indispensable source of information about core crimes and social media platforms have become “accidental archives”⁵, where “the information

³ Defined as in Article 5 of the ICC Rome Statute: the crime of genocide, crimes against humanity, war crimes, the crime of aggression.

⁴ FREEMAN Lindsay. Digital Evidence and War Crimes Prosecutions: The Impact of Digital Technologies on International Criminal Investigations and Trials. *Fordham International Law Journal*, volume 41, 2018, pp. 283-336; KHAN, Karim. Innovation and Technology in Building Modern Investigations and Prosecutions at the ICC. In: *The International Criminal Court in Its Third Decade. Reflecting on Law and Practices*. STAHN, Carsten; BRAGA DA SILVA, Rafael (eds.). Brill, 2023, pp. 102, 108-109.

⁵ DIGITAL LOCKERS: Archiving Social Media Evidence of Atrocity Crimes 2021, Human Rights Center, UC Berkeley School of Law (https://human-rights.berkeley.edu/sites/default/files/digital_lockers_report5.pdf), p. 10 (access 16.01.23).

posted on social media sites may include critical data for proving the core elements of crimes” – and in some cases may be the only documentation of such events⁶. Alongside the social media Internet-derived sources of evidence there are other sources as well; such as digital audio and video-recordings, CCTV footage, aerial and satellite imagery, drone footage etc. Among other Internet-stored and procedurally relevant data digital databanks and reports prepared by representatives of civil society are also of growing significance⁷. NGOs not only gather and store information about potential witnesses of crimes, but they also perform fact-checking and verification of the data sources – some of them also prepare reports on certain topics or events concerning war crimes or other core crimes; reports which can be used in a criminal investigation. Most of the data – acquired, processed, and presented publicly – can be easily accessed online. Such NGO-led investigations have thus become a *signus temporis* of the recent wars. Such was the case in the armed conflict in Syria, where the Syrian Archive and the Commission for International Justice and Accountability engaged in evidence collection and has been collecting and preserving social media videos and other online content documenting

⁶ DE ARCOS TEJERIZO, Maria. Digital evidence and fair trial rights at the International Criminal Court, *Leiden Journal of International Law*, Volume 36, Issue 3, September 2023, pp. 2-3; KOENIG, Alexa; MCMAHON, Felim; MEHANDRU, Nikita; SILLIMAN BHATTACHARJEE, Shikha. Open Source Fact-Finding in Preliminary Examinations. In: BERGSMO, Morten; STAHN, Carsten (eds.). *Quality Control in Preliminary Examination: Volume 2*, Torkel Opsahl Academic EPublisher, 2018, p. 683; MCDERMOTT, Yvonne; KOENIG Alexa; MURRAY, Daragh. Open Source Information's Blind Spot. Human and Machine Bias in International Criminal Investigations, *Journal of International Criminal Justice*, Volume 19, Issue 1, 2021, p. 87; MCPHERSON, Ella; GUENETTE THORNTON, Isabel; MAHMOUDI Matt. Open Source Investigations and the Technology-Driven Knowledge Controversy in Human Rights Fact-Finding. In: DUBBERLEY, Sam, KOENIG, Alexa, MURRAY, Daragh (eds.). *Digital Witness: Using Open Source Information for Human Rights Investigation, Documentation, and Accountability*, Oxford University Press, 2019, p. 74; MEHANDRU Nikita, KOENIG Alexa. Open Source Evidence and the International Criminal Court, *Harvard Human Rights Journal*, 15 April 2019, <https://harvardhrj.com/2019/04/open-source-evidence-and-the-international-criminal-court/> (access 16.01.23).

⁷ See e.g. MCGONIGLE LEYH, Brianne. Using Strategic Litigation and Universal Jurisdiction to Advance Accountability for Serious International Crimes, *The International Journal of Transitional Justice*, Volume 16, 2022, pp. 369-370.

the conflict⁸. In the case of the war in Ukraine, such evidence is gathered by numerous organisations, including among many others eyeWitness to Atrocities⁹ and Mnemonic¹⁰; the archives of which provide records from social media documenting alleged war crimes in Ukraine (in the so-called Ukrainian Archive);¹¹ by a Netherlands-based investigative journalism group called Bellingcat that specialises in fact-checking and open-source intelligence;¹² and the Conflict Observatory (functioning with the support of the Bureau of Conflict and Stabilization Operations of the United States Department of State); which was created in order to “capture, analyze, and make openly available the details of Russia-perpetrated war crimes and atrocities” in Ukraine¹³.

This text presents an analysis of how the ICC copes with this new digital environment of gathering evidence – and the chosen methodology for this will be analytical theoretical analysis. It is necessary to set the

⁸ See: FREEMAN Lindsay. Digital Evidence ... op.cit., p. 332; AKSAMITOWSKA, Karolina. Digital Evidence in Domestic Core International Crimes Prosecutions: Lessons Learned from Germany, Sweden, Finland and The Netherlands, *Journal of International Criminal Justice*, Volume 19, Issue 1, 2021, p 190.

⁹ eyeWitness | Welcome (accessed 10.07.24).

¹⁰ See the Mnemonic webpage <<https://mnemonic.org/en/our-work>>, (accessed 12.06.2024).

¹¹ ‘Digital Lockers: Archiving Social Media Evidence of Atrocity Crimes 2021, *Human Rights Center, UC Berkeley School of Law*, <https://humanrights.berkeley.edu/sites/default/files/digital_lockers_report5.pdf>, pp. 29-31 (access 11.07.24).

¹² TOLER, Aric. How we Geolocated a Photo of a Russian Missile Programming Team, *Bellingcat*, 28 October 2022, <<https://www.bellingcat.com/resources/2022/10/28/how-we-geolocated-a-photo-of-a-russian-missile-programming-team/>> (accessed 11.07.24).

¹³ For a thorough analysis of the reports presented by these organizations, see: KUCZYŃSKA, Hanna. Digital evidence in investigations concerning Russian crimes in Ukraine, in: GRZEBYK, Patrycja, UCZKIEWICZ, Dominika (eds.), *The Russian-Ukrainian Conflict and War Crimes. Challenges for Documentation and International Prosecution*, Routledge 2024 (forthcoming); CAIANIELLO, Michele. The Role of the EU in the Investigation of Serious International Crimes Committed in Ukraine. Towards a New Model of Cooperation?. *European Journal of Crime, Criminal Law and Criminal Justice*, Issue 30, Volume 3-4, 2022, pp. 219-237; examples of reports prepared by the Conflict Observatory: <https://hub.conflictobservatory.org/portal/apps/sites/#/home/pages/mariupol-1>, (accessed 11.07.24).

foundations for this analysis and point out the main characteristics of this specific digital environment in order to outline the picture of hardships and challenges that have to be met by the ICC. Firstly, this article analyzes the response of the Office of the Prosecutor (OTP) to the digital environment of gathering of evidence, where the OTP has decided to use algorithms in order to more effectively manage evidence. The digital tools harnessed in the pursuit of justice are the OTPLink and Project Harmony – which is considered to be “a milestone in the OTP’s wider technological upgrade”, under the motto: “To pursue justice more effectively, we must harness the power of cutting-edge technology. In today’s world, it is not a luxury, it is a requirement”¹⁴.

Secondly, the legal consequences of these new developments will be analyzed, as well as the dangers they pose for the assessment of evidence and the fact-finding process. In this part it will be necessary to establish whether this is indeed a “AI revolution”. Furthermore, the analysis will relate to answering the question whether the digitalized tools used by the OTP fulfill all the preconditions when it comes to providing for the credibility and authenticity of digital evidence.

The last part of the analysis will refer to the attitude to digital evidence adopted by the Chambers when it comes to the assessment of such evidence and fact-finding. It will be shown in this regard that it is necessary to distinguish between the case law of the Chambers, which relies on the traditional assessment of open sources; and the revolutionized algorithm-based gathering and management of evidence by the OTP. The key questions that need to be answered are whether the revolution is taking place only before the OTP, while the Chambers are adopting a more evolutionary attitude; whether this attitude is sufficient when it comes to the growing significance of digital evidence and the specific requirements of investigations into core crimes; and whether this is the attitude that we expect on the part of the ICC - and whether perhaps the ICC is not adequately developing new rules on the admission of evidence in light of the digital revolution ushered in by the OTP.

¹⁴ Statement of the ICC Prosecutor of 24.05.2023: ICC Prosecutor Karim A.A. Khan KC announces launch of advanced evidence submission platform: OTPLink | International Criminal Court ([icc-cpi.int](https://www.icc-cpi.int)), (accessed 11.07.24).

2. THE DIGITAL REVOLUTION IN THE WORK OF THE OTP

2.1. THE DIGITAL TRANSFORMATION OF PROSECUTORIAL TOOLS OF INVESTIGATION

In the increasingly digital environment of storing and presenting information about core crimes, the OTP decided to use algorithms in order to more effectively store and manage evidence. These algorithms were designed as tools to be used in order to automatize evidentiary proceedings at all stages of collecting, storing, securing, and analyzing evidence. The OTP Annual Report announced that: “This digital transformation is huge for us – it’s like stepping into the future where our tools are smarter and our skills are always up to date”¹⁵. This ‘digital transformation’ applied by the OTP consists of the digital application of referrals of crimes falling within the jurisdiction of the ICC (the OTPLink), and of developing a digital tool that allows to use algorithms to analyze and manage data (Project Harmony). The system – as it is planned and currently described – is supposed to harness the advanced technology and artificial intelligence in the pursuit of justice.

On the 23rd of May 2023 the Prosecutor announced the launch of the OTPLink application; allowing for online and email-based submissions of evidence to the OTP by all external stakeholders and witnesses. It replaces the multiple systems previously used under Article 15 of the Rome Statute (RS) to share submissions with the OTP. The OTPLink is designed with two distinct portals, enabling both anonymous and authenticated users (such as States Parties) to make submissions. In the words of the ICC Prosecutor Karim A.A. Khan: “This innovative application not only blends the use of advanced modern-day technology and international law; it provides users with a seamless and secure method for submitting potential evidence in real-time from any web-enabled device, effectively bringing relevant events closer to the courtroom”; and it should not only preserve the integrity of the evidence, but in the words of the makers it creates “a dependable and tamper-proof record of the collection and handling

¹⁵ Delivering Better – Office of the Prosecutor Annual Report 2023 (icc-cpi.int), p. 52, (accessed 11.07.24).

process”, and also allows to “handle larger information volumes utilizing Artificial Intelligence (AI) and Machine Learning (ML), significantly reducing the time required to review and act on it”.

The OTP Annual Report presents detailed data about the use of this digital web-based platform: as of 5 October 2023, the Office has received a total of 10.528 submissions through the OTPLink. Of those submissions, 48 have been registered as Article 15 RS submissions, while 99 were counted as evidence relevant to a situation. Furthermore, 693 were found to require further review by the Preliminary Examinations Section, and 9.687 submissions were characterized as general communications to the Office. The report informs readers that this online platform receives on average 100 to 150 submissions each day, and dedicated teams classify them in the categories described above, as well as by situation.

Project Harmony, apart from the OTPLink, includes components that will not only provide a centralised storage for information and evidence, but also integrate a range of investigative and analytical tools for secure use in the cloud. The OTP Annual Report describes the specific technology used in the Project. Firstly, eDiscovery technology software allows for secure, expansive and resilient data storage, and eVault ensures a secure environment for the permanent retention of electronic evidence (as the Office has moved from its previous online system and on-premises vault to this cloud-based storage). Secondly, the eVault provides centralized storage for information and evidence, allowing for the ingestion of electronic evidence that needs to be preserved; ensuring the digital preservation of evidence with systematic backups; allowing for capturing and management of contextual information; and ensuring a full audit trail. The whole system in its totality allows to elevate the capacities of the OTP in order to quickly analyze and manage larger quantities of evidence¹⁶.

¹⁶ Statement of the ICC Prosecutor of 24.05.2023: ICC Prosecutor Karim A.A. Khan KC announces launch of advanced evidence submission platform: OTPLink | International Criminal Court ([icc-cpi.int](https://www.icc-cpi.int)), (accessed 11.07.24). It should underlined though that this is not the first case of using such tools in investigations concerning core crimes – Europol and the European Union are using similar functionalities in the analysis of data: Core International Crimes Evidence Database (CICED) | Eurojust | European Union Agency for Criminal Justice Cooperation (europa.eu), (accessed 21.07.2024).

This enhancement relates to three areas of evidence-analysis and management. The first development is the technical analysis of data, including comparing biometric traits, e.g. facial identification, vocal recognition; image enrichment, multimedia file translations, automatic transcription (and transliteration); and video and image analysis (rapid pattern identification). While none of these innovations are new in themselves, when combined in this way they may prove invaluable to the OTP's effectiveness in collecting, storing, securing, analyzing, and reviewing evidence. For example, facial identification tools can help investigators obtain potential forensic versions by allowing them to more quickly compare multiple images that may show the same person¹⁷.

The second improvement is the management of data stored in the database. The algorithm is said to be able to easily filter out irrelevant information, allowing to focus on the most credible and relevant information¹⁸. Utilization of machine learning algorithms for tasks such as analyzing, transcribing, and processing video and audio materials is intended to "significantly condense the time frame of these processes – what used to take four to six weeks might now be accomplished within a few hours or minutes"¹⁹. The third improvement is a search-engine, allowing for targeted searches of source materials. Such a tool (although the report does not mention it) should also be able to cross-match the results of analyses.

Presently, Office of the Prosecutor Strategic Plan 2023-2025²⁰ describes in detail how the OTP intends to use new technologies to further

¹⁷ CRAWFORD, Julia; PETIT, Franck. Insights on the digital revolution for war crimes probes in Ukraine, *JusticeInfo.Net*, 31 May 2022 <<https://www.justiceinfo.net/en/93111-insights-digital-revolution-war-crimes-probes-ukraine.html>>, (accessed 10.05.24); EVANS, Hayley; HAZIM, Mahir. Digital Evidence Collection at the Int'l Criminal Court: Promises and Pitfalls OT-PLink, Project Harmony, and Digitalization Efforts, *JustSecurity*, July 5, 2023, <https://www.justsecurity.org/87149/digital-evidence-collection-at-the-intl-criminal-court-promises-and-pitfalls/>, (accessed 11.07.24).

¹⁸ Delivering Better – Office of the Prosecutor Annual Report 2023 (icc-cpi.int), (accessed 11.07.24).

¹⁹ Delivering Better – Office of the Prosecutor Annual Report 2023 (icc-cpi.int), (accessed 11.07.24).

²⁰ Office of the Prosecutor Strategic Plan 2023-2025, 2023-strategic-plan-otp-v.3.pdf (icc-cpi.int), (access 11.07.24).

revolutionize the performance of its processing tasks: e.g. Strategic Goal no. 3 is titled “Make the Office a global technology leader”. The OTP has announced that it “is seeking to revolutionize the use of technological tools in its work to enhance its ability to draw on digital, documentary, video and audio material.” Its goal is to “make the Office the global leader in the use of technology for accountability purposes”; with the first step being to establish and use the cloud-based e-Discovery platform. Another important element of the digital revolution is to ensure that staff members undertake a full training programme aimed at ensuring the effective harnessing of these new tools. Also, the Technology Advisory Board will be established, with new terms of reference and membership, which should provide effective strategic input to the development and implementation of actions under this strategic goal²¹. The strategic plan describes how the OTP will base its activities on “data enrichment/ analytical tools, including AI and machine-learning”; “with the support of a dedicated e-Discovery and Data Analysis Unit”.

2.2. MORE QUESTIONS THAN ANSWERS: EVALUATION OF THE LEGAL AND TECHNICAL FRAMES OF THE TECHNOLOGICAL REVOLUTION

The creation and involvement of both digital tools for data analysis – OTPLink and Project Harmony – is undoubtedly proof not only that the ICC has “entered the future”, but that the entire model of prosecuting international crimes should be re-evaluated. The use of the latest technology can ensure the ability of witnesses and victims of core international crimes to provide information and data on an unprecedented scale, and enable each victim to reach the ICC, which in turn increases the efficiency of managing this abundant evidence. It enables the OTP to strategically use limited resources and analyze large amounts and volumes of data and evidence at lower costs and in less time. At the same time however, it also forces participants to pose specific questions – questions that require much more information than the answers offered in the

²¹ MCINTYRE, Gabrielle; VIALLE, Nicholas. The Use of AI at the ICC: Should we Have Concerns? Part I, *Opinio Juris*, 11.09.23, The Use of AI at the ICC: Should we Have Concerns? Part I - *Opinio Juris*, (access 11.07.24).

above-cited OTP reports. In addition, the evaluation of this development must be presently based only on the reports of the OTP and the information provided by the Office – information which is very general in nature. It does not give an answer to the question whether any specific decision taken by the Office has been so far based on the AI-processed data. Moreover, the ‘automatic analysis’ of data is also supposed to “facilitate rapid decision making” – but there are no examples of what type of decision making this could be.

Firstly, there is the problem of defining the technical nature of Project Harmony. The question must be asked whether it is possible to claim that AI is actually being utilized by the OTP. While AI can be defined as “a set of theories and techniques used to create machines capable of simulating human intelligence”²², the process of management of evidence in Project Harmony is not fully automatic yet. There is nothing in the description of the OTP that would suggest that Project Harmony is making its own decisions or developing its own machine-learning techniques²³. Is it the description itself that is lacking this important element, or is there perhaps no such plan in the OTP? What we know is that there are automatic innovative algorithms, which can contribute in the search for evidence, their analysis, and management. It is clear that in this system algorithms play an important role. However, they do not take the place of humans as the entity making a decision. They do not fully control the procedure, but provide data and results of analyses; quickly analyzing big data and extracting information that can be useful to investigators and establishing correlations between pieces of information that are invisible to the human eye. Only when the first results of the work of these algorithms will be announced will it be possible to evaluate if the algorithms used by the OTP are indeed AI systems, and whether they can produce information suitable as evidence for use in ICC trials. In a situation when this information has not been revealed and there is no clear scope of automatic decision-making, it is hard to argue that certain decisions should be left in human hands (or at least that there should “human in the

²² https://www.larousse.fr/encyclopedie/divers/intelligence_artificielle/187257, (accessed 11.07.24).

²³ However, see: KHAN, Karim. *Innovation and Technology op.cit.*, p. 111.

loop” making the ultimate choices). Certainly, this an important element of this discussion on the use of AI in evidence management.

Secondly, the digital revolution in the ICC should not be limited solely to the OTP; it should extend to the whole of the ICC’s functioning. Therefore, the digitalization of the gathering and management of evidence should also extend to the methods of presentation in the courtroom, and become visible in the case law of the Chambers. Accordingly, the OTP is planning to “ensure improved results in the courtroom” which should be achieved by expansion of its technical capabilities and improvements in the management of investigations and prosecutions²⁴. The OTP report announces that “Embracing technology is vital for success”, but leaves it to the reader to guess what is meant by “success”. As a matter of fact, also the stage of the presentation of evidence by the OTP has definitely undergone a technological transformation. The new digital tool – the ICC Interactive Digital Platform – was designed for the presentation of evidence at the trial phase, providing a visual and spatial evidentiary model for cases. Such a digital platform, created by SITU Research, was first used in order to give a full picture of the places where core crimes had been committed in Timbuktu in the Mali situation²⁵. Later, after working closely with the OTP ICC on the *Al Mahdi* case in 2016, SITU Research was re-engaged by the ICC in 2018 to begin work on the *Al Hassan* case²⁶.

The Interactive Digital Platforms was used during the confirmation of charges hearing and throughout the trial itself. The prosecution displayed it on all the courtroom screens for the judges, witnesses, and audience members to see. This platform was used to walk the judges through the crimes *Al Mahdi* and *Al Hassan* had been charged with, enabling navigation to the site of the crime and, when available, displaying footage of the accused committing the alleged crimes. The camera used in the courtroom made it possible to shift into the viewpoint of the photograph or video, such that the footage integrated within the digital model was

²⁴ Delivering Better – Office of the Prosecutor Annual Report 2023 (icc-cpi.int), § 23 (accessed 11.07.24).

²⁵ SITU Research: ICC Digital Platform: Timbuktu, Mali, SITU – ICC Digital Platform: Timbuktu, Mali (accessed 15.07.24).

²⁶ SITU – ICC Digital Platform and the *Al Hassan* Case (accessed 21.07.2024).

seamless. However, in the case law of the ICC Chambers little is seen or discussed about these achievements.

2.3. ALGORITHMIC BIAS AND DEEPPAKES – POTENTIAL DANGERS OF DATA-ANALYSIS

The second set of problems stems from the risks typical for the use of algorithms in data-analysis. The first such risk is the bias built into the algorithms; the second – feeding the algorithm with intentionally falsified data²⁷. Serious concerns are expressed in the literature relating to the fact that the analysis of evidence performed by an algorithm must assume that the algorithm is properly focused on the specific data sets in question and in accordance with the appropriate specific patterns. As a result, the acquired analysis may be susceptible to “algorithm bias” (e.g. in relation to racial, ethnic or gender issues). For example, in the case of facial recognition systems, the model may be trained on less diverse data sets and lead to inaccurate and biased recognition of people of a nationality or race whose representatives are more likely to commit crimes. Gender bias may also occur due to gaps in the documentation regarding harm to men and women, due to social norms²⁸. Algorithmic systems can only be as good as the data they are trained on. That is why the scope and nature of the data fed to the algorithm is crucial. Therefore, a diverse set of training data, error mitigation techniques, and regular evaluation of the machine learning model should be employed in order to mitigate these risks. In this regard, the words of the Prosecutor Karim A.A. Khan can be helpful in establishing that such risks have been taken into consideration and prevented: “eDiscovery platforms allow advanced and detailed data analytics and searching, assisting with the prevention or detection of unconscious bias which impacts the work of investigators and analysts. The use of an evidence life-cycle management

²⁷ EVANS, Hayley; HAZIM, Mahir. Digital Evidence Collection ... op.cit., (accessed 11.07.24).

²⁸ MIMRAN, Tal; WEINSTEIN, Lior. Digitalize It: Digital Evidence At the ICC, *Lieber Institute West Point*, 14.08.23, Digitalize It: Digital Evidence at the ICC - Lieber Institute West Point, (accessed 11.07.24).

system in conjunction with an eDiscovery platform may provide a macro-level overview of the sources, geographical distribution, and language distribution of available evidence”²⁹.

Given the context in which the algorithms operate, another potential problem is the possibility of feeding them with fake data, which can lead to misclassification of examples. For instance, a machine learning model may be intentionally misled to incorrectly classify or identify an object or person. In the era of deepfakes, small, intentional data disruptions cannot be ruled out. Every photo, every video and digitally stored information can be predisposed to be false. Also, large amounts of data may be created intentionally, which may lead to the creation of a false narrative – these may be campaigns sponsored by states or private entities pursuing specific goals³⁰. Deepfakes can be created not only manually, but they can be also created by Generative AI – a term that refers to “any tool based on a deep-learning software model that can generate text or visual content based on the data it is trained on”. There are even special tools available online for this purpose; tools that have emerged in recent years and are “capable of generating images realistic enough to create disinformation”³¹. Such intentional disinformation could involve, for example, digitally replacing a specific uniform with another, or changing a face to look like another person’s face. The creators of Project Harmony should anticipate such eventualities and constantly improve the analysis algorithms. When digital sources of information (as well as the OTPLink) are fed disinformation, the mere threat or suspicion of information modification can lead to undermining the very possibility of obtaining evidence in this way, thus negating its procedural value for fact-finding³².

²⁹ KHAN, Karim. *Innovation and Technology ...op.cit.*, p. 120.

³⁰ MIMRAN, Tal; WEINSTEIN, Lior. *Digitalize It: Digital Evidence At the ICC, Lieber Institute West Point*, 14.08.23, *Digitalize It: Digital Evidence at the ICC - Lieber Institute West Point*, (accessed 11.07.24).

³¹ It is called AI or Not (drag and drop application) - advanced algorithms and machine learning techniques that analyse images and detect signs of AI generation. The AI was trained on DALL-E, Midjourney, Stable Diffusion, generative adversarial networks and face image generators, see: *AI or Not | AI Detector to Check for AI in Images & Audio* (accessed 11.07.24).

³² EVANS, Hayley; HAZIM, Mahir. *Digital Evidence Collection ... op.cit.*, (accessed 11.07.24).

Finally, it is important to note that Project Harmony was built in cooperation with IT external entities. A description of their contribution is available in the report on the activities of the Prosecutor's Office. The OTP partners became "Microsoft and Accenture/Avanade, which provided support in designing and building infrastructure; implementing security measures; and management". The OTP addresses this, stating that "while safeguarding its independence and the confidentiality of its work, this partnership has allowed the Office to benefit from technical and industry-specific skills and capabilities". This Project was also financed by a grant from the European Union, whose aim was to "introduce a modern, efficient evidence management system and develop artificial intelligence and machine learning tools to analyse and process data"³³. Although such support from external entities is an interesting solution from the point of view of cooperation between diverse actors in the prosecution of international crimes, it also poses new questions as to the independence of these private actors and their influence in the ICC actions. The question that should be asked with respect to the stage of entering into this partnership is how far the activities of the ICC may influence this relationship. For the time being it is important to bear in mind that the physical storage of the data in Project Harmony is on the U.S. territory. It is debated whether this solution may prove sensitive given current developments – especially in terms of, *inter alia*, probability of issuing arrest warrants charging top Israeli officials of core crimes³⁴.

3. ASSESSMENT AND EVALUATION OF ALGORITHM-MANAGED AND ANALYZED EVIDENCE BY THE ICC

3.1. RULES OF VERIFICATION OF DIGITAL EVIDENCE

The last question relates to the quality of Project Harmony-stored and managed data when it comes to the standards of verification

³³ All citations after: Report of the Committee on Budget and Finance on the work of its thirty-ninth session, CC-ASP/21/15, 29 November 2022, ICC-ASP-21-15-ENG.pdf (icc-cpi.int), § 245, (accessed 11.07.24).

³⁴ AKSENOVA, Marina. All Eyes on the International Criminal Court, *LAW Global Affairs*, 17.07.24, <https://www.ie.edu/insights/articles/all-eyes-on-the-international-criminal-court/> (accessed 11.07.24).

of digital evidence in general. There is a need to verify the authenticity and evidential value of any digital data before they may become evidence in trial³⁵. Verification should become an obligatory stage in criminal investigations, allowing for the accuracy of the source and validity of a piece of evidence to be established³⁶.

The first problem related to using digital evidence is verification of the method of preservation of digital data: digital preservation is an important aspect to ensure authenticity and credibility³⁷. As rightly observed in the literature on this topic, it is necessary “to ensure the integrity of the evidentiary material and preserve the history of its transmission through continuous instrumental controls during data retrieval”. Moreover, “any action taken on electronic evidence must be documented so that an independent third party can repeat the action and obtain a similar result”³⁸. This problem should be solved by Project Harmony. The OTP

³⁵ BRAGA DA SILVA, Rafael. Updating the Authentication of Digital Evidence in the International Criminal Court, *International Criminal Law Review*, Volume 22, Issue 5-6, 2021, pp. 941-964; QUILLING, Chelsea, The Future of Digital Evidence Authentication at the International Criminal Court, *Journal of Public and International Affairs*, 20.05.2022, <https://jpia.princeton.edu/news/future-digital-evidence-authentication-international-criminal-court>, (accessed 11.07.24).

³⁶ AIDP resolution: section 3 – AI and the administration of criminal justice: ‘Predictive policing,’ ‘predictive justice,’ and evidence, Buenos Aires, 28–31 March 2023, AIDP RESOLUTIONS. Section 3.pdf (penal.org) (access 21.07.2024).

³⁷ MOLINA GRANJA, Fernando; RODRIGUEZ Glen Dario. The Preservation of Digital Evidence and Its Admissibility in the Court, *International Journal of Electronic Security and Digital Forensics*, Volume 9, 2017, writing about the Long Term Digital Preservation (LTDP), which is the set of processes, strategies and tools used to store and access digital data for long periods of time during which technologies, formats, hardware, software and technical communities are very likely to change <https://www.researchgate.net/publication/312934498_The_preservation_of_digital_evidence_and_its_admissibility_in_the_court>, (accessed 11.07.24). See also: RUGGIERI, Franco. Security in digital data preservation, *Digital Evidence and Electronic Signature Law Review*, Volume 11, 2014, p. 100-102.

³⁸ BLAHUTA, Roman; MOVCHAN, Anatolii; MOVCHAN, Maksym. Use of Electronic Evidence in Criminal Proceedings in Ukraine, *Advances in Social Science, Education and Humanities Research. Proceedings of the International Conference on Social Science, Psychology and Legal Regulation*, 18.11.21, p.

states that “eDiscovery technology software allows for secure, expansive, and resilient data storage”; and eVault functionality ensures “a secure environment for the permanent retention of electronic evidence”.

The second stage of verification should be identification of the source. There are several software products that help to obtain information about the owner of the domain (site); his/her IP address; and find out where the server with the site (hosting or colocation) is located; there are also free services on the Internet that can be used to get information about the resources of the network (sites). As part of verifying the authenticity of information, it is also possible to identify the source of information in the digital environment, e.g. by using programs that help obtain information about the owner of the domain (website), its IP address, and find out where the server is located (hosting or colocation, e.g. using IP-Tools; SmartWhois, Mod IP City³⁹). It is however not clear whether Project Harmony deals with these problems: i.e. whether one of the algorithms included in the Project has such a task; or verification of the source will be executed by a “human factor”: an OTP investigator or an expert called by the Court, potentially at the request of the defence. Undoubtedly, every piece of information stored and analyzed in the database should be provided with references regarding its source.

It is only from the Prosecutor that the observer can learn about the technicalities of the Project and become convinced that both verification of the source and the highest standards of credibility are taken care of: “The ELMS manages evidence through its entire lifecycle and assures that all relevant evidence is collected and stored in a manner consistent with international standards. This begins at the source, tracking all source development, investigations, forensics, e-discovery and analysis tasks. ELMS captures evidence intake and registration, including by investigators in the field using its companion mobile application. In keeping with the highest international standards, ELMS reliably documents the chain-of-custody in an auditable format and records the location of physical and

198, Use of Electronic Evidence in Criminal Proceedings in Ukraine | Atlantis Press (atlantis-press.com) (accessed 11.07.24).

³⁹ See: BLAHUTA, Roman; MOVCHAN, Anatolii; MOVCHAN, Maksym. Use of Electronic Evidence in Criminal ...op.cit., pp. 197-200.

digital evidence”⁴⁰. Another problem, however, is establishing the real author of the information – anonymous evidence being posted online should be certainly tracked to the real author, in order to ascertain its credibility, regardless of tracing it back to the person who made it available on the web or in the OTPLink.

Later, as the fourth stage of analysis, digital evidence must be properly managed. There is too much data and too many unknown factors to let such evidence be entered into the record without any standards. Here too some NGO digital applications allow for the management of data, like, e.g., the eyeWitness to Atrocities. In other cases NGOs assign data to concrete events, using geolocation and chronolocation techniques (e.g. Amnesty International). This task should be fulfilled by Project Harmony – it promises to “use cloud computing capabilities to review large quantities of complex information and evidence”⁴¹. It should also be able also to easily filter out irrelevant information, making it possible to focus on the most credible and relevant information.

3.2. “POST-TRUTH” AND DISINFORMATION

Another problem is that ‘in a “post-truth” world, the camera often lies’⁴². Every piece of digital evidence should be checked for possible fakes. Thus, the next stage of processing digital evidence is verification of the authenticity of the digital data. This can be done by internal investigators or algorithms – checking the data by following available sources and links. In the case law of the ICC, it turns out that usually experts are called in order to verify the veracity of data. Such verification can be executed in different ways. The methods for doing so are various, all rooted in the digital environment: they can include comprehensive metadata checks, reverse image searches, as well as more sophisticated tools and techniques,

⁴⁰ KHAN, Karim. Innovation and Technology ...op.cit., pp. 111-112.

⁴¹ Delivering Better – Office of the Prosecutor Annual Report 2023 (icc-cpi.int), (accessed 11.07.24).

⁴² D’ALESSANDRA, Federica; SUTHERLAND, Kirsty. The Promise and Challenges of New Actors and New Technologies in International Justice, *Journal of International Criminal Justice*, Volume 19, Issue 1, 2021, p. 24.

making it possible to reveal potential tampering, misattribution, and authorship and authenticity. Another issue is who should be responsible for this verification phase: external or internal experts. Certainly, if experts are called they should be “persons with specialized skills and knowledge in this domain, who can testify with regard to its provenance, reliability, and authenticity”⁴³. The question arises however whether they should be parties, experts appointed by parties, or independent experts called by the ICC? There is no such functionality in this regard mentioned in the description of Project Harmony. Secondly, it is possible that law enforcement agencies could apply technological solutions capable of discovering deepfakes without a need to call an expert⁴⁴.

At the same time, the ICC’s procedural framework governing expert evidence is very limited and certainly was not designed for application to OSINT. There is no clear answer as to which type of specialized knowledge will be accepted as expert evidence for OSINT materials, which is especially visible when it comes to the array of technical analyses the ICC has used so far. The literature points out that there is no sign that any objective criteria for calling a specific expert witness have yet been adopted, as before the ICC the expert status is accorded to a small number of typically privileged individuals based on relatively opaque assessments⁴⁵. In *Al Hassan* case, the video analysis expert was called in order to analyze images and geolocate them. However, the Prosecutor instructed the expert that he may use also “any other means” in case of “trouble” conducting the geolocation. The instructions lacked any more specific information on whether these “other means” should

⁴³ GILLET, Mathew; FAN, Wallace. Expert Evidence and Digital Open Source Information Bringing Online Evidence to the Courtroom, *Journal of International Criminal Justice*, Volume 21, Issue 4, 2023, p. 673. KOENIG, Alexa; FREEMAN, Lindsay. Cutting-Edge Evidence: Strengths and Weaknesses of New Digital Investigation Methods in Litigation, *Hastings Law Journal*, Volume 73, 2022, p. 1235.

⁴⁴ GARRIE, Daniel B.; MORRISSY, David J. Digital Forensic Evidence in the Courtroom: Understanding Content and Quality, *Journal of Technology and Intellectual Property*, Volume 12, Issue 2, 2014, p. 122.

⁴⁵ GILLET, Mathew; FAN, Wallace. Expert Evidence ... op.cit., p. 679.

include searching for other images or materials, and, if so, how those searches should be preserved and documented – and whether at all⁴⁶.

An important role when it comes to the verification of evidence is clearly played by civil society. Verification of the authenticity of materials available in the Internet was done, e.g., by Bellingcat. Such verification techniques have proven to be successful, as seen in connection with the downing of Malaysian Airline flight MH17 in Ukraine in 2014⁴⁷. Cross-checking of open source information, comparing videos and images of the scene with Google Maps and other similar tools, along with analysis of social media data to identify the weapon used and link the incident to Russian involvement, the Bellingcat investigators proved that “Russia’s Ministry of Defense had manipulated geospatial imaging related to the downing of Malaysian Airlines flight MH17, including altering the terrain, removing the presence of Russian military vehicles, and obscuring important features of the airplane crash site with fake clouds”⁴⁸. In another report from 29 March 2023 the Bellingcat team established that available online evidence presented as digital data, i.e. a dash-camera video of Ukrainian soldiers harassing woman, was staged⁴⁹.

It is also possible to authenticate the information from the side of the providers of such information. The authors of the footage or users can themselves ensure the evidentiary value of digital evidence (*a priori*), using one of many digital applications (like the eyeWitness to Atrocities application linking the photos and videos with metadata)⁵⁰.

⁴⁶ GILLET, Mathew; FAN, Wallace. Expert Evidence... op.cit., p. 673.

⁴⁷ MH17 - The Open Source Evidence - bellingcat (accessed 21.07.2024). What is interesting, in the ECHR case *Ukraine and The Netherlands vs Russia* (applications nos. 8019/16, 43800/14 and 28525/20, judgment of 30 November 2022, in the case of Malaysian Airline flight MH17 the Court unequivocally supported the admission of digital visual evidence as “credible and serious” against the arguments by lawyers representing Russia – referring, among others, to this specific report of Bellingcat.

⁴⁸ QUILLING, Chelsea, *The Future of Digital Evidence ...op.cit.*; UMBERG, Tommy; WARDEN, Cherrie. *Digital Evidence and Investigatory Protocols, Digital Evidence and Electronic Signature Law Review*, Volume 11, 2014, p. 128.

⁴⁹ *How Online Investigators Proved Video of Ukrainian Soldiers Harassing Woman was Staged* - bellingcat, (accessed 15.07.2024).

⁵⁰ eyeWitness | Welcome, (accessed 10.07.24).

Summarising this line of argument, comparison of the standards for providing for credible and authentic digital evidence and the presently known model of operation of Project Harmony leads to the conclusion that the question whether the standards of verification of digitally acquired evidence are provided in the frames of Project Harmony cannot be answered, due to insufficient amount of data on the functioning of this Project.

3.3. PROCEDURAL FRAMEWORK OF THE ICC FOR SUBMITTING DIGITAL EVIDENCE

In the procedural framework of the ICC, the only rules for processing digital evidence result from Regulation 26 of the Regulations of the Court⁵¹. These rules are supposed to provide for a reliable, secure, and efficient electronic system which supports its daily judicial and operational management and its proceedings. In this system, documents, decisions and orders shall, whenever possible, be submitted in electronic version for registration by the Registry. A very detailed description of formal requirements for the presentation of evidence has been provided. Along with Article 69 of the Statute, and Regulation 26, the so-called Unified Technical Protocol (“E-court Protocol”), was also introduced, whose procedural function is to transmit evidence and witness and victim information to the Court in electronic form⁵². It is designed to ensure that all the necessary information is available electronically to the Court during the proceedings. The Protocol defines the standards according to which the participants should prepare and provide evidence, potential evidence, and material in electronic form. Furthermore, the Protocol defines the metadata which should accompany the materials submitted. These standards are designed to minimise the document management and technology costs to the participants and the Court and to allow for the efficient management of proceedings. Evidence and material

⁵¹ Available online: RegulationsCourt_2018Eng.pdf (icc-cpi.int), (accessed 10.07.24).

⁵² Unified Technical protocol, ICC-01/14-01/18-64-Anx 23-01-2019, CR2019_00267.PDF (icc-cpi.int), (accessed 10.07.24).

that a participant intends to submit to a Chamber in a hearing, can be processed by the Court's electronic system and must comply with the system's standards.

By way of example, the Protocol requires that all digital files sent to the electronic system were provided with a digital signature; that is a unique cryptographic code that is "generated for an electronic item that may be used to verify the authenticity of evidence in the event its authenticity is challenged". Digitized "video information should display time codes that reflect the full duration of the content that is contained in the original media. Where an entire video cannot be provided during disclosure, and in exceptional circumstances, then an excerpt may be provided. Any video excerpt should display the original time-coding so that it is possible to associate it to scenes from the original complete video" (§ 29 of the Protocol).

The literature recognizes the advantages of introducing digital tools for managing the delivery of evidence to the Court, but it also states that the Protocol should be systematically reviewed by cybersecurity experts for previously unnoticed security gaps, and adjusted to prevent the possibility of compromising its security on an ongoing basis⁵³.

4. ASSESSMENT AND EVALUATION OF DIGITAL EVIDENCE IN THE ICC CASE LAW

4.1. INTERNET-DERIVED EVIDENCE IN THE ICC COURTROOM

The case law of the ICC Chambers does not yet show the results of the algorithmic revolution (announced only last year). The jurisprudence of the ICC since 2010 has shown that factual findings have been based on digital evidence from open sources and the Internet environment in general. Judicial practice indicates that data obtained online, from social media, and data obtained during their analysis using chrono-location and geo-location have become indispensable tools in conducting proceedings

⁵³ MORIARTY, Kathleen. Why Are Authentication and Authorization So Difficult? Center for Internet Security. October 18, 2021. Why Are Authentication and Authorization So Difficult? (cisecurity.org), (accessd 11.07.24).

in cases of core international crimes⁵⁴. However, even though digital evidence has been widely presented by the prosecution before the ICC, no procedural rules have been adopted by the ICC Chambers as to their credibility and admissibility, nor are there any rules specially dedicated to checking the authenticity of evidence. They have rather pointed to the need to use a holistic assessment of such evidence, based on their relevance to a case; thus balancing their credibility versus their significance. In order to assess the scope of the use of digital evidence, it is necessary to examine what type of evidence was used by the prosecution and what consequences such evidence has had on the ICC's factual findings.

In the hearing on the confirmation of charges in the cases of *Prosecutor v. Abu Garda*⁵⁵ and *Prosecutor v. Saleh Jerbo Jamus*⁵⁶, the prosecution presented satellite imagery, which has played an important role in tracking the burning and destruction of villages; the movement of populations; and the location of the aircrafts used by the Government of Sudan⁵⁷. In 2018 the arrest warrant against Mahmoud Mustafa Busayf Al-Werfalli was based in large part on video footage of executions found on social media websites. The ICC Pre-Trial Chamber admitted the videos as evidence, explaining that it was “satisfied that the above mentioned video has sufficient indicia of authenticity in order to be relied upon at this stage of the proceedings. The Chamber noted in particular that the Prosecutor had submitted an expert report on the authentication of the video, prepared by a renowned, independent institute. Having analysed the video and its key frames, the report concluded that there were no traces of forgery or manipulation in relation to the locations, weapons, or persons shown in the video. The location was also confirmed by a witness”⁵⁸. However, this case did not progress to trial due to the reported death of the suspect.

⁵⁴ FREEMAN Lindsay. Digital Evidence ... op.cit., pp. 289-290.

⁵⁵ *Prosecutor v. Bahr Idriss Abu Garda* Public, ICC-02/05-02/09-243-Red, Decision on the Confirmation of Charges, 8.02.2010.

⁵⁶ *Prosecutor v. Abdallah Banda Saleh Jerbo Jamus*, ICC-02/05-03/09-121-Corr-Red, Decision on the Confirmation of Charges, 7.03.2011.

⁵⁷ FREEMAN Lindsay. Digital Evidence ... op.cit., p. 306.

⁵⁸ *The Prosecutor v. Mahmoud Mustafa Busayf Al-Werfalli*, Second Warrant of Arrest, ICC-01/11-01/17, 4.07.2018, § 18.

In 2016, the *Prosecutor v. Al Mahdi* case became best known for the amount of digital evidence presented by the prosecution⁵⁹. Besides witness statements, satellite images from Google Earth – both from before and after the destruction of buildings – were presented, as well as archive photographs taken at different times; audio recordings found on the Internet containing statements from members of armed groups; and videos from YouTube recordings on the Internet, which showed the destruction at the time of the attack. Digital tools of verification were also used: the investigators used geolocating tools to find the locations presented in the open source videos and photographs. In this case the prosecution used both internal investigators to verify the authenticity of the images by geolocating the landmarks in the images collected from YouTube, and publicly available digital images found on the Internet. They also used external experts – including a geolocation report from an expert witness which made it possible to “locate with certainty” each video with regard to a precise mausoleum; as well as relying on an expert report ascribing dates and a time frame to the videos in order to present 360-degree panoramic photographs⁶⁰. The defence did not object to the use of such digital evidence and tools, so there was no need to decide on the admissibility of such material. The expert evidence was not challenged, as the parties stipulated that they would not offer evidence or submissions inconsistent with the plea agreement⁶¹. However, even this extraordinary utilization of open sources and digital technology did not lead to a groundbreaking sentence based mainly on such digital evidence; the Al-Mahdi conviction was largely based on his guilty plea and accompanying confession⁶².

In contrast, in the 2015 *Prosecutor v. Bemba* case the defense argued that the photographs the investigators found on Facebook – which

⁵⁹ *Prosecutor v. Ahmad Al Faqi Al Mahdi*, ICC-01/12-01/15-171, Judgment and Sentence, 27.09.2016.

⁶⁰ FREEMAN Lindsay. Digital Evidence ... op.cit., pp. 316-317.

⁶¹ Agreement regarding admission of guilt, Al Mahdi, Annex 1, ICC-01/12-01/15-78-Anx1-tENG-Red, Office of the Prosecutor and Defence, 25.02.2016, CR2016_06550.PDF (icc-cpi.int) (accessed 21.07.2024), § 14.

⁶² GILLET, Mathew; FAN, Wallace. Expert Evidence ... op.cit., p. 686; HELL-WIG, Kristina. The Potential and the Challenges ...op.cit., p. 667.

were used to link individuals and corroborate other evidence – were not *prima facie* authentic or reliable, as the Prosecution provided no material supporting the attribution of the Facebook photos. They pointed out the fact that “since the creation of a Facebook account does not require any valid identity information, it is impossible to forensically ascertain, even on a *prima facie* basis, that a Facebook account under a certain name is attributable to a person of the same name”. Secondly, the photographs were not genuine extracts but merely screenshots of a webpage with a pop-up photograph. The defence argued that, “unlike a genuine extract, the metadata of the photograph, such as the creation date, the photographing device, and the modification traces were not available, which warranted their exclusion”. Such information is particularly relevant since the photographs were used in conjunction with events on a particular date. Thirdly, it was argued that the photographs had no probative value at this juncture, and thus the identification of the persons in the images was not yet evidence. In the opinion of the defence, the prosecution also failed to provide any explanation or justification as to why this material was not being tendered through a witness⁶³.

In response, the Trial Chamber decided that it would not make any ruling on the relevance and/or admissibility of the 1,028 items of evidence submitted by the prosecution at that time beyond its previous decisions taken under Article 69(7) RS. It stated that “there is no reason for the Chamber to make admissibility assessments in order to screen itself from considering materials inappropriately. The notion of a fair trial does not require that the Chamber rule on the admissibility of each piece of evidence upon submission”⁶⁴. Finally, the Trial Chamber did not address the admissibility of the photographs from Facebook either in its final judgment, since they were not deemed relevant to its decision,

⁶³ The Prosecutor v. Jean-Pierre Bemba Gombo, Aimé Kilolo Musamba, Jean-Jacques Mangenda Kabongo, Fidèle Babala Wandu And Narcisse Arido; Public Redacted Version of Defence Response to Prosecution’s Third Request for the admission of Evidence from the Bar Table, ICC-01/05-01/13-1170, 9.10.2015, § 83-86.

⁶⁴ Decision on Prosecution Requests for Admission of Documentary Evidence, ICC 01/05-01/13-1013-Red, ICC-01/05-01/13-1113-Red, ICC-01/05-01/13-1170-Conf, 24.10.2015, § 12.

“thus kicking the can down the line to future Chambers to decide on the admissibility of social media photos, perhaps in a case where they play a more significant role in directly proving the elements of the crimes”⁶⁵.

In none of the above-cited cases did the Chamber implement any strict rules concerning the admissibility of digital evidence. In accordance with Rule 63(2) of the Rules of Procedure and Evidence (RPE), on each occasion it freely assessed all the evidence submitted in order to determine its relevance or admissibility. It decided not to make *prima facie* individualized rulings on the admissibility of each item of evidence submitted during the course of the proceedings, other than on the basis of any procedural bars such as those under Article 69(7) RS or concerning the procedural requirements for the introduction of prior recorded testimony under Rule 68 RPE⁶⁶. The Chamber thus assessed the relevance, probative value, and potential prejudice of all the submitted evidence in a holistic manner. Arguments as to their admissibility raised by the defence in the course of the trial were decided in the context of the final judgment, as part of its holistic assessment of all the evidence. No atomistic rules of admissibility of evidence were thus used or established.

4.2. WITNESSES' TESTIMONIES AS REGINA PROBATIONUM?

A similar attitude was visible in the most recent case decided by the ICC Trial Chamber. In its judgment of 26 June 2024, the Trial Chamber convicted Al Hassan⁶⁷ of the charges brought against him of war crimes and crimes against humanity committed between 2 April 2012 and 29

⁶⁵ FREEMAN Lindsay. Digital Evidence ... op.cit., p. 328.

⁶⁶ See e.g. The Prosecutor v. Al Hassan Ag Abdoul Aziz Ag Mohamed Ag Mahmoud, Trial Judgment, 26.06.2024, ICC-01/12-01/18, § 23-24; Judgment on the appeal of Mr Jean-Pierre Bemba Gombo against Trial Chamber III's "Judgment pursuant to Article 74 of the Statute", ICC-01/05-01/08-3636-Red, 8.06.2018, § 53; § 105; The Prosecutor v. Bosco Ntaganda, ICC-01/04-02/06-2359, Trial Judgment, 8.07.2019, § 48-53; The Prosecutor v. Dominic Ongwen, Trial Judgment, ICC-02/04-01/15-1762-Red, 4.02.2021, § 249.

⁶⁷ The Prosecutor v. Al Hassan Ag Abdoul Aziz Ag Mohamed Ag Mahmoud, Trial Judgment, 26.06.2024, ICC-01/12-01/18.

January 2013 in Timbuktu, northern Mali, controlled at that time by the armed groups Ansar Dine and Al-Qaida in Islamic Maghreb (AQIM). It results from the judgment that the Chamber based several of its factual findings on Facebook evidence: such as the social circumstances and reality in places where the criminal acts were committed – especially when it came to facts relating to the residents of Timbuktu enjoying freedoms in terms of social activity and religious practice (§ 413-414) and the proclamation of an independent state called Azawad (§ 452). The Chamber's decision was also based on posts of witnesses proving the guilt of the suspects (§ 734) and the general opinion of the local society about the suspects (§ 1070). All Internet-derived information was considered to play only a supportive role, as corroborating evidence (although this notion was not used by the Chamber), whereas the decisive evidence on which fact-finding was based came from witnesses.

However, it is hard to make definitive statements, as the text of the trial judgment mentions on many occasions videos and photos; although without being precise about their origins, or whether they were found in a digital environment. Such an attitude hinders the possibility to confirm the existence of any definitive rules with respect to the admissibility of such evidence. Nonetheless, this attitude may at the same time indicate to an outside observer that once evidence is uploaded in the digital system of submission of evidence, their provenance loses importance and is not conclusive for the assessment of credibility or significance. One should also keep in mind that basing fact-finding on digital evidence may be perceived as a “short-cut” version of achieving justice, as there is no more reliable and valuable evidence than hearing the oral testimonies of eyewitnesses, who can be cross-examined. The quantity of witnesses' testimonies that the Chamber based their decision on would, when compared to other evidence, seem to confirm this attitude. The Chamber gave a clear priority to the oral testimonies of the witnesses over the advantages that the digital environment of evidence-gathering may have brought for the case. On the other hand this attitude ignores the growing variety of types of evidence.

In consequence, this case also proved that academics awaiting a digital revolution in the case law of the Chambers when it comes to rules of admissibility of digital sources of evidence must remain disappointed.

Based on its previous case law, the Chamber decided that in order “to fulfil its obligation to provide a reasoned opinion” under Article 74(5) of the Statute, “it is not required to address all the arguments raised by the parties [and participants], or every item of evidence relevant to a particular factual finding, provided that it indicates with sufficient clarity the basis for its decision”⁶⁸. It confirmed that trial chambers have a degree of discretion and flexibility about what to address explicitly in their reasoning, so long as they provide sufficient reasons for their determinations. The arguments of the defence were addressed in the text of the reasoning before turning to the factual findings, when specific types of evidence were discussed and assessed. Several of these arguments related to digital sources of information.

The defence argued that one of the witnesses, who testified about the existence of a plan to launch a series of assaults on the Malian State positions in the northern part of the country, could not be relied upon to establish the existence of hostilities as “his information was gleaned from Internet searches and impacted by inappropriate steers from the Prosecution”⁶⁹. The Chamber stated that this argument was only based “on one portion of a transcript related to one question asked by the Prosecution during a prior interview of the witness”, and that this witness gave a clear and plausible explanation to this question. In doing so the provenance of this information from the Internet was used in order to misrepresent the witness’ testimony on these issues as a whole. Thus in this case the information given by the witness was assessed to be relevant and directly arising from the witness’s observations. Another argument of the defence related to an incident when members of the Islamic Police arrested two men in Timbuktu for consuming alcohol, who were later brought to the Islamic Court by members of Ansar Dine/AQIM and were sentenced for drinking alcohol and flogged. This information was based on an article available on the Internet. However, the Chamber stressed that the circumstances of this event were confirmed by eye witnesses and

⁶⁸ The Prosecutor v. Al Hassan Ag Abdoul Aziz Ag Mohamed Ag Mahmoud, Trial Judgment, 26.06.2024, ICC-01/12-01/18, § 32.

⁶⁹ The Prosecutor v. Al Hassan Ag Abdoul Aziz Ag Mohamed Ag Mahmoud, Trial Judgment of 26.06.2024, ICC-01/12-01/18. Reference 1137, p. 178.

therefore, even though depending on the parameters of the computer the date of the article sometimes changed when the file was transferred or published on the Internet and saved again, this evidence had no bearing on the Chamber's conclusion about the circumstances of the case⁷⁰. In consequence, witnesses' testimonies remained overwhelming in volume as evidentiary material and conclusive for the Chamber's fact-finding.

4.3. THE MODEL OF HOLISTIC EVALUATION OF EVIDENCE

The last part of the analysis relates to the influence of the digital form of presentation of evidence on the final judgment (or more precisely, the lack of thereof). In preparing evidence for Al Hassan trial, the OTP employed a digital tool for presenting evidence designed by SITU Research, containing an interactive replica of the city that included visual evidence of where the alleged crimes took place, combining videos of drone footage, satellite imagery, laser scans, 3D data, panoramic images and geospatial data; all of which required the integration and interoperability of a broad range of assets. "Because the alleged crimes were committed in various locations across Timbuktu, the virtual model was designed to allow the Prosecution, Defense, and Judges to navigate the city and gain a comprehensive understanding of these events in both time and space"⁷¹. Also, the prosecution introduced a video analysis expert to use digital evidence and platforms such as Google Earth to geolocate monuments in the Timbuktu area in Mali as the basis for creation of this platform.

However, there is no mention about the use of such an advanced digital tool in the reasoning of the judgment, which raises the question whether this was actually a piece of evidence at all, or just a tool for presenting evidence⁷². From the description available online (as

⁷⁰ The Prosecutor v. Al Hassan Ag Abdoul Aziz Ag Mohamed Ag Mahmoud, Trial Judgment, 26.06.2024, ICC-01/12-01/18, § 762.

⁷¹ SITU – ICC Digital Platform and the Al Hassan Case (access 21.07.2024).

⁷² See on that topic and the lack of equality of arms, as the defense teams for the accused lack the same resources offered to the prosecution: ELLIOT, Victoria. War Crimes Prosecutions Enter a New Digital Age, *Wired*, 26.06.2024, War Crime Prosecutions Enter a New Digital Age | WIRED, (access 11.07.24).

cited above) it results that it was not a piece of evidence: “it is both to support contextualization (to help strengthen witness testimony) and corroboration (to show that evidence was taken in the purported locations). Specifically, the digital model allowed the judges and other parties unable to travel to Timbuktu to contextualize the alleged crimes. This approach is particularly helpful in this case as the security situation in Mali remains poor, precluding any possibility of the judges visiting the sites in person”; adding that: “The platform has been used as the primary vehicle to present video and photographic evidence”. It seems that the concept was to visualize and display the previously available pieces of evidence, and not the introduction of evidence itself in the procedural meaning of the term. Notably, this attitude was confirmed by both the prosecution and defence, as the defence did not challenge the use of the platform, provided that all evidence presented therein would be admitted into evidence separately⁷³. Indeed, the defense sought full access to the virtual platform, and required (and was provided with) training and guidance on its use, so that they could also deploy it as needed⁷⁴.

At the same time it is necessary to keep in mind the dangers and prejudice that such a digital presentation of evidence brings with it: “digital reconstructions can be so easily believed to be true even if there is a significant possibility for human bias or error, this technology needs to be approached with caution through a critical lens when used in international criminal courtrooms in order for justice to be progressed and not hindered”⁷⁵. It is worth noting that all the data presented in the digital platform had been confirmed on the ground by, *inter alia*, a technical reconnaissance mission that was conducted for the Prosecution in

⁷³ And by KHAN, Karim. Innovation and Technology op.cit., p. 106.

⁷⁴ KHAN, Karim. Innovation and Technology ... op.cit., p. 107.

⁷⁵ ZARMSKY, Sarah. Why Seeing Should Not Always Be Believing: Considerations Regarding the Use of Digital Reconstruction Technology in International Law, *Journal of International Criminal Justice*, Volume 19, Issue 1, 2021, p. 221; MCDERMOTT, Yvonne; MURRAY, Daragh; KOENIG, Alexa. Digital Accountability Symposium: Whose Stories Get Told, and by Whom? Representativeness in Open Source Human Rights Investigations, *Opinio Juris*, 19.12.19, Digital Accountability Symposium: Whose Stories Get Told, and by Whom? Representativeness in Open Source Human Rights Investigations - *Opinio Juris*, (accessed 21.07.2024).

Timbuktu in June 2013 with a view to studying the damage that occurred to some monuments and examining other sites, including two mosques and six mausoleums (§ 1030 of the trial judgment); as well as the calling of a specialist on satellite imagery and geospatial data analysis, who conducted a satellite imagery analysis of locations of interest – namely mausoleums and monuments – in Timbuktu (§ 1031).

To recapitulate, the Court decided to adopt the model of carrying out a holistic evaluation of the totality of evidence presented (or revealed) in the case in order to determine its relevance and meaning for the case in the last stage of evaluation, that is after the trial and the presentation of all the evidence. It is characteristic of the continental model of a criminal trial that the totality of the evaluation of evidence takes place not during atomistic, *a priori* evaluation, but during the holistic stage of evaluation. This model assumes that there is no need for formal rules or an *a priori* evaluation of evidence: both as to its credibility and its relevance⁷⁶. On the continent it is believed that it is not possible to decide *a priori*, at the level of a legal act, about the relevance and credibility of evidence⁷⁷. As professionals, fact-finders do not have to be protected by numerous rules regarding the admissibility of evidence, as they can professionally assess the relevance and credibility and the weight of the evidence offered. From the continental point of view, the alternative would signify shifting the “decision-making centre” from the level of the free assessment of a judge to the level of a legal act. Apparently the ICC follows this model.

This does not mean that the holistic approach excludes the possibility to undermine the evidentiary value of digitally acquired evidence. There is much criticism in the literature when it comes to the weaknesses of such an attitude, and specific standards are being mentioned that the ICC disregarded. Insofar as regards the *Al-Mahdi* case, reasonable reservations

⁷⁶ HO, Hock Lai. The Fair Trial Rationale for Excluding Wrongfully Obtained Evidence. In: Do Exclusionary Rules Ensure a Fair Trial?: A Comparative Perspective on Evidentiary Rules, GLESS, Sabine; RICHTER, Thomas (eds.). Basel: Springer 2019, p. 288.

⁷⁷ DAMAŠKA, Mirjam. Evidence Law Adrift, Yale University Press, 1997, p. 20; KUCZYŃSKA, Hanna. Mechanisms of elimination of undesired evidence from criminal trial, *Brazilian Journal of Criminal Procedure*, Volume 1, 2021, pp. 43-92.

have been made in the literature as to the reliability of the verification methods used on OSINT materials. Authors have pointed to the fact that digital tools are not 100% credible and the defence may easily undermine their credibility via an expert opinion. For example, it is possible to challenge the admission of Google Earth images, particularly if they are presented by the prosecution in the format of a screenshot⁷⁸, which is a final result of certain software techniques. At the same time the process of getting to this final result should be acknowledged and assessed in the light of its impact on the credibility of such a screenshot. In the literature it is proposed that the verification stage could include: seeking out the raw images from Google; questioning employees of Google Earth about their process; or verifying on the ground the accuracy of the satellites used by Google Earth in that location and time⁷⁹. Based on the accuracy of a given satellite, it can be proven that Google Earth's positional accuracy is not fixed, but rather varies from one time to another – which can also be the result of the process of uploading and updating images; a process which involves periodically replacing old images with more recent or better resolution images. It can also be the result of shaping three-dimensional pictures into sphere. This observation leads to the conclusion that the “reliability of Google Earth images and the extracted positional data should be supported with field checks of the locations, and corroborated by other evidence”⁸⁰.

In consequence, it should be suggested that the model of evaluation of evidence should be “activated”; whether by “modernization” of the presently existing system simply by interpreting the existing legal provisions Article 69(7) differently or by adding a new rule of procedure. When it comes to the first option, Article 69(7) RS is so broad in its wording that it leaves room for a different (non-holistic) interpretation that could be presented in the caselaw of the Court. A new hermeneutical line of assessment of the admissibility of evidence, regarding e-evidence, could be worked out, in which the weighing of credibility would be a

⁷⁸ See: GRIMM, Paul; CAPRA, Daniel, JOSEPH, Gregory. Authenticating Digital Evidence, *Baylor Law Review*, Volume 69, 2017, pp. 35-36; MCDERMOTT, Yvonne; KOENIG Alexa; MURRAY, Daragh. Open Source Information's Blind Spot ... op.cit., p. 87.

⁷⁹ As rightly proposed by: FREEMAN Lindsay. Digital Evidence ... op.cit., p. 328.

⁸⁰ As rightly proposed by: FREEMAN Lindsay. Digital Evidence ... op.cit., p. 328.

necessary condition for admissibility. The second option would require a change in the Rules of Procedure and Evidence, which is a more tedious and risky undertaking, leading to less flexible results.

7. CONCLUSIONS

When the ICC commenced operations in 2002, the digital age was in its infancy⁸¹. The present stage of technological development is the consequence of the significant technological advancements of everyday life and the need to adjust the potential of the OTP to the needs of the social life that has so rapidly become digital. The main question asked in the text relates to how the ICC adapted itself to this digital age. The answer to this question had to be divided into several lines of argumentation, as there are various layers of analysis that appear when it comes to the digital revolution before the ICC. The practice of the ICC regarding digital evidence, and specifically open sources evidence, shows how many questions arise from the use of digital evidence and digital tools of analysis. There are many challenges that OSINT-based evidence has introduced to the paradigm of assessment of evidence, including the lack of an established and formalized system of their verification⁸².

The first layer of analysis was thus the technological revolution: technology is a key accelerator of the OTP's work when it comes to the gathering and analysis of evidence. As was explained earlier in the text, the Office has embarked on a monumental digital transformation, a clear indication of its commitment to integrating state-of-the-art technologies into its operations⁸³. Does this mean that a sort of "AI investigation" has been brought to life? This text in the first place has demonstrated that this cannot be stated beyond doubt. In the second place - it has listed the dangers that come with this development. The conclusion of the text is therefore that there should be rules governing the use of algorithms used in the analysis and management of data; rules known to the parties and the

⁸¹ GILLETT, Mathew; FAN, Wallace. Expert Evidence ... op.cit., p. 691.

⁸² GILLETT, Mathew; FAN, Wallace. Expert Evidence ... op.cit., p. 661

⁸³ Delivering Better – Office of the Prosecutor Annual Report 2023 (icc-cpi.int), (accessed 11.07.24).

judges, in order to provide for sufficient transparency in the functioning of the pattern of analysis and predictability of the criteria used by the algorithm. Moreover, the special role and position of the defence should be taken into consideration, as obviously there is no possibility to cross-examine the algorithm in order to gain information about how it evaluated the data.

The second part of this analysis led to the conclusion that under the ICC's current procedures, there is no established normative framework specifically governing the admission of evidence acquired in a digital environment, or any other type of digital data⁸⁴. At the same time, the use of open source evidence in light of the ICC practice has been vigorously debated in the literature, which has pointed out several flaws in the presently-existing solutions. The problem is that the ICC has not decided about the need for the existence of rules governing the admissibility of digital evidence; instead quite freely adopting various methods of verification to a given piece of evidence and information. The Chambers have not even replied to the question concerning the taxonomical categorization of online sources used, i.e. whether it was documentary evidence; real evidence; a mixture of the two, or maybe testimonial evidence. The presently reigning lack of stable rules obviously provides for flexibility whereby judges can adapt the assessment of evidence to the different needs of every case. But still this model of assessment should fulfill the conditions regarding transparency and accessibility⁸⁵. This approach is described in the literature as a “minimalist and flexible approach”, and often criticized; especially in the Anglo-Saxon literature⁸⁶. However, there is no doubt that there is a need to establish standards that are clear, accessible, objectively justifiable, and non-biased for the admission of such evidence⁸⁷. These do not necessarily have to be

⁸⁴ See also: GILLET, Mathew; FAN, Wallace, Expert Evidence ... op.cit., pp. 661–693.

⁸⁵ WILLE, Belkis.” Video Unavailable”: Social Media Platforms Remove Evidence of War Crimes, *Human Rights Watch*, 10.09.20, <https://www.hrw.org/report/2020/09/10/video-unavailable/social-media-platforms-remove-evidence-war-crimes>, (accessed 10.07.24).

⁸⁶ GILLET, Mathew; FAN, Wallace, Expert Evidence ... op.cit., pp. 661–693.

⁸⁷ GILLET, Mathew; FAN, Wallace, Expert Evidence .. op.cit, p. 686; HELLWIG, Kristina. The Potential and the Challenges of Digital Evidence in International Criminal Proceedings, *International Criminal Law Review*, Volume

written standards. Such standards of verification, authenticity and the credibility of digital evidence can also be established in the ICC case law.

As a result of the current approach, no new procedural rules have appeared or been adopted before the ICC, even though the sources and methods of digital gathering of evidence have changed dramatically since 2002, especially when the first OSINT materials became part of the evidentiary material. At the same time, admitting digital evidence into a criminal trial involving core crimes became crucial and indispensable. Despite the emergence of a totally new level of the technological revolution in the gathering and analysis of evidence; and later in the method of preparation of evidence by the prosecution for presentation in the Court; there has been no revolution in the rules of admissibility and assessment of such evidence. Should there be one? At this moment the logical and academic answer would seem to be yes, but it is visible from the practice of the ICC that this is not necessarily the case. The Chambers in trial judgments have chosen to make use of the traditional tools for the evaluation and analysis of evidence, where the main fact-finding is based on “traditional” types of evidence. This attitude does not seem to be sufficient when it comes to the growing significance of digital evidence and the specific requirements surrounding the investigation into core crimes and the need to accommodate the new challenges appearing with the introduction of Project Harmony. It seems that the ICC is not adequately developing new rules on the admission of evidence in light of the digital revolution ushered in by the OTP. This does not mean that there is a need for a totally new model of assessment of evidence, but only that such a model should exist. Moreover, the less human control there is over the algorithms that analyze the data, the more judicial control there should be over the methods and results of such analysis.

LIST OF BIBLIOGRAPHICAL REFERENCES

AKSAMITOWSKA, Karolina. Digital Evidence in Domestic Core International Crimes Prosecutions: Lessons Learned from Germany, Sweden, Finland and The Netherlands, *Journal of International Criminal Justice*, Volume 19, Issue 1, 2021.

22, issue 5-6, 2021, p. 982; STOYKOVA, Radina, Digital Evidence: Unaddressed Threats to Fairness and the Presumption of Innocence, *Computer Law and Security Review*, Volume 42, 2021, p. 12.

AKSENOVA, Marina. All Eyes on the International Criminal Court, *LAW Global Affairs*, 17.07.24, <https://www.ie.edu/insights/articles/all-eyes-on-the-international-criminal-court/>.

BLAHUTA, Roman; MOVCHAN, Anatolii; MOVCHAN, Maksym. Use of Electronic Evidence in Criminal Proceedings in Ukraine, *Advances in Social Science, Education and Humanities Research. Proceedings of the International Conference on Social Science, Psychology and Legal Regulation*, 18.11.21, Use of Electronic Evidence in Criminal Proceedings in Ukraine | Atlantis Press (atlantis-press.com).

BRAGA DA SILVA, Rafael. Updating the Authentication of Digital Evidence in the International Criminal Court, *International Criminal Law Review*, Volume 22, Issue 5-6, 2021.

CAIANIELLO, Michele. The Role of the EU in the Investigation of Serious International Crimes Committed in Ukraine. Towards a New Model of Cooperation?. *European Journal of Crime, Criminal Law and Criminal Justice*, Issue 30, Volume 3-4, 2022.

CRAWFORD, Julia; PETIT, Franck. Insights on the digital revolution for war crimes probes in Ukraine, *JusticeInfo.Net*, 31 May 2022 <<https://www.justiceinfo.net/en/93111-insights-digital-revolution-war-crimes-probes-ukraine.html>>.

D'ALESSANDRA, Federica; SUTHERLAND, Kirsty. The Promise and Challenges of New Actors and New Technologies in International Justice, *Journal of International Criminal Justice*, Volume 19, Issue 1, 2021.

DAMAŠKA, Mirjam. Evidence Law Adrift, Yale University Press, 1997.

DE ARCOS TEJERIZO, Maria. Digital evidence and fair trial rights at the International Criminal Court, *Leiden Journal of International Law*, Volume 36, Issue 3, 2023.

ELLIOT, Victoria. War Crimes Prosecutions Enter a New Digital Age, *Wired*, 26.06.2024, War Crime Prosecutions Enter a New Digital Age | WIRED.

EVANS, Hayley; HAZIM, Mahir. Digital Evidence Collection at the Int'l Criminal Court: Promises and Pitfalls OTPLink, Project Harmony, and Digitalization Efforts, *JustSecurity*, 5.07.2023, <https://www.justsecurity.org/87149/digital-evidence-collection-at-the-intl-criminal-court-promises-and-pitfalls/>.

FREEMAN Lindsay. Digital Evidence and War Crimes Prosecutions: The Impact of Digital Technologies on International Criminal Investigations and Trials. *Fordham International Law Journal*, Volume 41, 2018.

GARRIE, Daniel B.; MORRISSY, David J. Digital Forensic Evidence in the Courtroom: Understanding Content and Quality, *Journal of Technology and Intellectual Property*, Volume 12, Issue 2, 2014.

GILLET, Mathew; FAN, Wallace. Expert Evidence and Digital Open Source Information Bringing Online Evidence to the Courtroom, *Journal of International Criminal Justice*, Volume 21, Issue 4, 2023.

GRIMM, Paul; CAPRA, Daniel, JOSEPH, Gregory. Authenticating Digital Evidence, *Baylor Law Review*, Volume 69, 2017.

HELLWIG, Kristina. The Potential and the Challenges of Digital Evidence in International Criminal Proceedings, *International Criminal Law Review*, Volume 22, Issue 5-6, 2021.

HO, Hock Lai. The Fair Trial Rationale for Excluding Wrongfully Obtained Evidence. In: Do Exclusionary Rules Ensure a Fair Trial?: A Comparative Perspective on Evidentiary Rules, GLESS, Sabine; RICHTER, Thomas (eds.). Basel: Springer 2019.

KHAN, Karim. Innovation and Technology in Building Modern Investigations and Prosecutions at the ICC. In: The International Criminal Court in Its Third Decade. Reflecting on Law and Practices. STAHN, Carsten; BRAGA DA SILVA, Rafael (eds.). Brill, 2023.

KOENIG, Alexa; FREEMAN, Lindsay. Cutting-Edge Evidence: Strengths and Weaknesses of New Digital Investigation Methods in Litigation, *Hastings Law Journal*, Volume 73, 2022.

KOENIG, Alexa; MCMAHON, Felim; MEHANDRU, Nikita; SILLIMAN BHATTACHARJEE, Shikha. Open Source Fact-Finding in Preliminary Examinations. In: BERGSMO, Morten; STAHN, Carsten (eds.). Quality Control in Preliminary Examination: Volume 2, Torkel Opsahl Academic EPublisher, 2018.

KUCZYŃSKA, Hanna. Digital evidence in investigation concerning Russian crimes in Ukraine, in: GRZEBYK, Patrycja, UCZKIEWICZ, Dominika (eds.), The Russian-Ukrainian Conflict and War Crimes. Challenges for Documentation and International Prosecution, Routledge 2024 (forthcoming);

KUCZYŃSKA, Hanna. Mechanisms of elimination of undesired evidence from criminal trial, *Brazilian Journal of Criminal Procedure*, Volume 1, 2021.

MCDERMOTT, Yvonne; KOENIG Alexa; MURRAY, Daragh. Open Source Information's Blind Spot. Human and Machine Bias in International Criminal Investigations, *Journal of International Criminal Justice*, Volume 19, Issue 1, 2021.

MCDERMOTT, Yvonne; MURRAY, Daragh; KOENIG, Alexa. Digital Accountability Symposium: Whose Stories Get Told, and by Whom? Representativeness in Open Source Human Rights Investigations, *Opinio Juris*, 19.12.19, Digital Accountability Symposium: Whose Stories Get Told, and by Whom? Representativeness in Open Source Human Rights Investigations - Opinio Juris

MCGONIGLE LEYH, Brianne. Using Strategic Litigation and Universal Jurisdiction to Advance Accountability for Serious International Crimes, *The International Journal of Transitional Justice*, Volume 16, 2022.

MCINTYRE, Gabrielle; VIALLE, Nicholas. The Use of AI at the ICC: Should we Have Concerns? Part I, *Opinio Juris*, 11.09.23, The Use of AI at the ICC: Should we Have Concerns? Part I - *Opinio Juris*.

MCPHERSON, Ella; GUENETTE THORNTON, Isabel; MAHMOUDI Matt. Open Source Investigations and the Technology-Driven Knowledge Controversy in Human Rights Fact-Finding. In: DUBBERLEY, Sam, KOENIG, Alexa, MURRAY, Daragh (eds.). *Digital Witness: Using Open Source Information for Human Rights Investigation, Documentation, and Accountability*, Oxford University Press, 2019.

MEHANDRU Nikita, KOENIG Alexa. Open Source Evidence and the International Criminal Court, *Harvard Human Rights Journal*, 15 April 2019, <https://harvardhrj.com/2019/04/open-source-evidence-and-the-international-criminal-court/>.

MIMRAN, Tal; WEINSTEIN, Lior. Digitalize It: Digital Evidence At the ICC, *Lieber Institute West Point*, 14.08.23, Digitalize It: Digital Evidence at the ICC - Lieber Institute West Point.

MOLINA GRANJA, Fernando; RODRIGUEZ Glen Dario. The Preservation of Digital Evidence and Its Admissibility in the Court, *International Journal of Electronic Security and Digital Forensics*, Volume 9, 2017, <https://www.researchgate.net/publication/312934498_The_preservation_of_digital_evidence_and_its_admissibility_in_the_court>.

MORIARTY, Kathleen. Why Are Authentication and Authorization So Difficult? Center for Internet Security. October 18, 2021. Why Are Authentication and Authorization So Difficult? ([cisecurity.org](https://www.cisecurity.org)).

QUILLING, Chelsea, The Future of Digital Evidence Authentication at the International Criminal Court, *Journal of Public and International Affairs*, 20.05.2022, <https://jpia.princeton.edu/news/future-digital-evidence-authentication-international-criminal-court>.

RUGGIERI, Franco. Security in digital data preservation, *Digital Evidence and Electronic Signature Law Review*, Volume 11, 2014.

STOYKOVA, Radina, Digital Evidence: Unaddressed Threats to Fairness and the Presumption of Innocence, *Computer Law and Security Review*, Volume 42, 2021.

TOLER, Aric. How we Geolocated a Photo of a Russian Missile Programming Team, *Bellingcat*, 28 October 2022, <<https://www.bellingcat.com/resources/2022/10/28/how-we-geolocated-a-photo-of-a-russian-missile-programming-team/>>.

UMBERG, Tommy; WARDEN, Cherrie. Digital Evidence and Investigatory Protocols, *Digital Evidence and Electronic Signature Law Review*, Volume 11, 2014.

WILLE, Belkis." Video Unavailable": Social Media Platforms Remove Evidence of War Crimes, *Human Rights Watch*, 10.09.20, <https://www.hrw.org/report/2020/09/10/video-unavailable/social-media-platforms-remove-evidence-war-crimes>.

ZARMSKY, Sarah. Why Seeing Should Not Always Be Believing: Considerations Regarding the Use of Digital Reconstruction Technology in International Law, *Journal of International Criminal Justice*, Volume 19, Issue 1, 2021.

Authorship information

Hanna Kuczyńska. Dr hab., professor at the Institute of Law Studies of the Polish Academy of Sciences in Warsaw, Criminal Law Department. hkuczynska@gmail.com

Additional information and author's declarations (scientific integrity)

Acknowledgements: The research project was financed from the funds of the National Centre of Science (Narodowe Centrum Nauki) granted on the basis of a contract No. UMO-2023/49/B/HS5/02623 for a project entitled "In search of justice for core crimes in the digital age."

Conflict of interest declaration: the author confirms that there are no conflicts of interest in conducting this research and writing this article.

Declaration of authorship: all and only researchers who comply with the authorship requirements of this article are listed as authors; all co-authors are fully responsible for this work in its entirety.

Declaration of originality: the author assures that the text herein published has not been previously published in any other resource and that future republication will only take place with the express indication of the reference of this original publication; she also attests that there is no third party plagiarism or self-plagiarism.

Editorial process dates

(<https://revista.ibraspp.com.br/RBDPP/about>)

- Submission: 21/07/2024
- Desk review and plagiarism check: 30/07/2024
- Review 1: 12/08/2024
- Review 2: 02/09/2024
- Preliminary editorial decision: 28/09/2024
- Correction round return: 21/10/2024
- Final editorial decision: 23/10/2024

Editorial team

- Editor-in-chief: 1 (VGV)
- Reviewers: 2

HOW TO CITE (ABNT BRAZIL):

KUCZYŃSKA, Hanna. The ICC enters into the future: the digital-evidence revolution or evolution? *Revista Brasileira de Direito Processual Penal*, vol. 10, n. 3, e1073, set./dez. 2024. <https://doi.org/10.22197/rbdpp.v10i3.1073>



License Creative Commons Attribution 4.0 International.