Leiden Journal of International Law (2023), **36**, 749–769
doi:10.1017/S0922156523000031

ORIGINAL ARTICLE

INTERNATIONAL CRIMINAL COURTS AND TRIBUNALS

Digital evidence and fair trial rights at the International Criminal Court

María de Arcos Tejerizo[1]

Pérez-Llorca Abogados - Litigation and Arbitration Department
Email: arcostej.maria@gmail.com

Abstract

International criminal proceedings are witnessing an increase in the use of digital sources of evidence at trial, and it is expected that digital evidence will shape the outcome of upcoming decisions of international criminal tribunals. Digital footage may arguably enhance the efficiency of international crimes investigations. However, the high expertise required to access, analyse, and assess digital materials may widen the gap between the prosecution and the defence, thus undermining fair trial rights. This article examines, in the context of proceedings before the International Criminal Court, the impact that the overreliance on digital evidence may have on the principle of equality of arms, and how such a situation might be alleviated.

Keywords: digital evidence; equality of arms; fair trial rights; International Criminal Court; open-source investigations

1. Introduction

Technology and digital communications have reshaped the way in which mass atrocities are investigated, prosecuted, and assessed by international criminal tribunals. New fact-finding methods, which may include reliance on digital open-source information, are assisting international courts and tribunals in building the narrative of international criminal accountability. At the outset of the Russian invasion of Ukraine, Ukrainian officials, local civil society groups, human rights organizations, and organizations devoted to forensic investigations began with the collection and preservation of digital media and other evidentiary material in Ukraine for the purposes of documenting war crimes.[2] These initial findings, if adequately used, will be key to establish criminal accountability for the commission of international crimes in Ukraine.

Digital documentation of international crimes has already played a role in proceedings before international criminal tribunals. In 2016, Al Mahdi pleaded guilty before the International Criminal Court (ICC) upon the overwhelming evidence introduced against him for the war crime of destruction of cultural property in Timbuktu (Mali).[3] The documentary evidence presented included satellite images and video recordings retrieved from the internet which, coupled with

[1]The views expressed in this article are those of the author and do not necessarily reflect the views of the author's affiliated institution. The author is solely responsible for the content of this article, and the institution is not responsible for any errors or omissions. This article is intended for academic purposes only and should not be taken as the institution's position on the topic.

[2]J. Hendrix, 'Ukraine May Mark a Turning Point in Documenting War Crimes', *Just Security*, 28 March 2022, available at www.justsecurity.org/80871/ukraine-may-mark-a-turning-point-in-documenting-war-crimes/.

[3]*The Prosecutor v. Ahmad Al Faqi Al Mahdi*, Judgment and Sentence, ICC-01/12-01/15, 27 September 2016.

geolocation reports, linked him with the destruction of certain mausoleums.[4] On the other hand, in the *Ayyash et al.* case before the Special Tribunal for Lebanon (STL), the prosecution heavily relied on mobile communications and geolocation data to prove that the co-defendants had tracked and planned the attack in Beirut on 14 February 2005 that killed former Lebanese Prime Minister Hariri and 21 others.[5] This required the procurement of vast amounts of call data records retrieved from either telecom providers or via co-operation with the Lebanese authorities.[6]

Digital evidence may be defined as 'information stored or transmitted in binary form that may be relied on in court'.[7] It may be obtained, among others, from a computer hard drive, from mobile phone telecommunications, from a flash card in a digital camera, or from open sources of information such as media outlets or the internet. However, not all forms of digital information may be used as evidence in court, for it is required that the information be reliable and have sufficient probative value.

While digital sources of information may contribute to bringing more direct and robust pieces of evidence to international criminal proceedings as compared to other types of evidence, e.g., witness testimonies, international institutions and the parties to the case may also encounter major difficulties when dealing with this kind of evidence. Standardized rules on the collection, preservation, and assessment of digital evidence are still at an embryonic stage, and thus its authority and reliability may be disputable. Further, the analysis and interpretation of digital data often demand specific software tools and expertise that international criminal tribunals usually lack. Lastly, judges and parties to the proceedings may not have adequate understanding of how the digital evidentiary materials are relevant to the facts of the case. These contingencies may lead to a biased and misleading evaluation of their probative value and, overall, to a disbalanced treatment towards the parties involved in the proceedings.

The literature relating to the use of digital evidence in international criminal proceedings has primarily focused on the legal standards of evidence applicable when investigating international crimes through digitally-derived evidence and open-source information. More precisely, the UC Berkeley Protocol on Digital Open Source Investigations (Berkeley Protocol) has brought together the standards and guidelines for investigators and civil society on the identification, collection, preservation, verification, and analysis of digital open-source information, in order to guarantee its effective use in international criminal and human rights investigations.[8] On their part, the Leiden Guidelines on the Use of Digitally-Derived Evidence in International Criminal Courts and Tribunals (Leiden Guidelines) have outlined the essential elements that practitioners should consider before submitting digitally-derived evidence to an international court or tribunal.[9] However, none of the existing literature has addressed how the increasing reliance on digital evidence in court may undermine fair trial rights in international criminal proceedings.

Accordingly, this article aims at examining the procedural challenges brought by the introduction of digital evidence in international criminal proceedings before the ICC, how this factor may lead to a disbalance in the equality of arms, and how the existing practices may be enhanced in light of the increasing reliance on digital evidence in court. Section 2 will provide an overview on

[4]L. Freeman, 'Digital Evidence and War Crimes Prosecutions: The Impact of Digital Technologies on International Criminal Investigations and Trials', (2018) 41 *Fordham International Law Journal* 283, at 316.

[5]*The Prosecutor v. Salim Jamil Ayyash*, Sentencing Judgment, STL-11-01/S/TC, 11 December 2020, paras. 11–27, 43, 140.

[6]*The Prosecutor v. Salim Jamil Ayyash et al.*, Decision on Appeal by Counsel for Mr. Oneissi against the Trial Chamber's Decision on the Legality of the Transfer of Call Data Records, STL-11-01/T/AC/AR126.9, 28 July 2015, paras. 3–4.

[7]M. Novak, J. Grier and D. Gonzales, 'New Approaches to Digital Evidence Acquisition and Analysis', (2019) 280 *National Institute of Justice Journal*, at 1.

[8]New York and Geneva, Human Rights Center and OHCHR, Berkeley Protocol on Digital Open Source Investigations: A Practical Guide on the Effective Use of Digital Open Source Information in Investigating Violations of International Criminal, Human Rights and Humanitarian Law (2020).

[9]Kalshoven-Gieskes Forum, Leiden University, *Leiden Guidelines on the Use of Digitally Derived Evidence in International Criminal Courts and Tribunals* (2021).

https://doi.org/10.1017/S0922156523000031 Published online by Cambridge University Press

how digital evidence has reshaped international criminal investigations and how this might be relevant for its potential use in international criminal proceedings, as compared to other large bodies of evidence. Section 3 will establish the impact and challenges that the collection, preservation, analysis, admissibility, and assessment of digital evidence in court brings in light of the principle of equality of arms. Lastly, Section 4 will shed light on the practices that might be put in place to guarantee equal procedural opportunities when relying on digital evidence in court. Overall, this article will advocate for a proactive role of the institutions and a more inquisitorial role of the Chambers to level off any possible prejudice that may be caused to the rights of the accused when confronting the use of digital evidence.

2. The relevance of digital evidence for international criminal investigations

Modern-day conflicts leave a digital footprint that is hard to destroy or lose trace of. The metadata contained in satellite imagery, intercepted communications, or photographs and videos may allow investigators to trace the content back to the date, time, geolocation, and authorship of the item of digital materials. If well-collected, verified and preserved, digitally-derived evidence may offer greater potential for the conduct of criminal investigations in conflict zones than other types of evidence.

To understand how digitally-derived evidence may be useful for criminal investigations and prosecutions, this section will discuss: first, what makes digital evidence different from other large bodies of evidence (Section 2.1); and second, how investigations of international crimes may benefit from the use of digital evidence, as opposed to other types of evidentiary materials (Section 2.2).

2.1 Preliminary remarks on how digital evidence differs from other large bodies of relevant evidence

The term 'digitally-derived evidence' encompasses both (i) evidence 'taken from and created by digital devices and via technology', such as cameras or satellites; and (ii) digitalized evidence, i.e., analogue materials that have been transferred to a digital format.[10] The processing of the latter type of digitally-derived evidence is regulated by the ICC E-Court Protocol.[11] However, this section mainly focuses on the former kind of digitally-derived evidence and, particularly, on open-source digital evidence.

Access to digital evidence usually requires seeking authorization, consent, or a judicial order whenever private or personal data are involved, or when the source of evidence can only be reached through coercive measures.[12] On its part, open-source information is publicly available information that may be accessed through observation, request, or purchase,[13] without need of seeking a judicial order or employing coercive measures.[14] This kind of information may come

[10]K. Orlovsky and A. Roche-Mair, 'Evidence Matters in ICC Trials', (2016) *International Bar Association*, at 19 (IBA Report).

[11]The ICC E-Court Protocol was designed to guarantee that 'all the necessary information is available electronically during the proceedings to the Court'. See *The Prosecutor v. Thomas Lubanga Dyilo*, Consolidated E-Court Protocol, ICC-01/04-01/06, 4 April 2008, Ann.

[12]For instance, in the *Bemba et al.* case, bank records from Western Union were considered admissible after the Chamber examined that they had been obtained via judicial order and that their collection complied with Austrian law requirements. See *The Prosecutor v. Jean-Pierre Bemba Gombo, Aimé Kilolo Musamba, Jean-Jacques Mangenda Kabongo, Fidèle Babala Wandu and Narcisse Árido*, Appeal Brief filed by the Defence for Jean-Jacques Mangenda Kabongo with the Appeals Chamber, ICC-01/05-01/13, 15 May 2017, para. 87.

[13]N. Mehandru and A. Koenig, 'Open Source Evidence and the International Criminal Court', *Harvard Human Rights Journal*, 15 April 2019, available at www.harvardhrj.com/2019/04/open-source-evidence-and-the-international-criminal-court/.

[14]A. Koenig, 'The New Forensics: Using Open Source Information to Investigate Grave Crimes', *Human Rights Center*, 1 July 2018, at 7, available at humanrights.berkeley.edu/publications/new-forensics-using-open-source-information-investigate-grave-crimes (HRC Report 2018).

https://doi.org/10.1017/S0922156523000031 Published online by Cambridge University Press

from different sources, in various forms, and may serve for wide-ranging purposes.[15] Social media posts, media outlets, or footage publicly shared by ordinary citizens, may all amount to open sources of evidence. Human rights activists and organizations may use online content to carry out fact-finding investigations and to elaborate their own reports on the events taking place in conflict zones.[16]

Some pieces of digital evidence, e.g., photographs or communication intercepts, may fall under the broad definition of documentary evidence.[17] However, evidence with a digital component has certain features that make it different from other large bodies of physical evidence, whether it be documentary, forensic, or witness testimony.

When reflecting on the uniqueness of digital evidence, the following considerations come to the fore:

1. First, the collection of digital evidence often involves a skill set different from physical evidence.[18] Sometimes, investigators do not have direct technical access to digital evidence, so they need to resort to public or private entities to ask for their co-operation to access the data. An example of this might be the need to request telecom operators for information for tracking IP addresses, or to ask social media service providers for sharing internally accessible information that had been previously deleted from the platform.[19] In some other cases, digital information is publicly available, as may be the case of open-source evidence, so the source of the evidence may be easily accessed by the investigator, or provided by private entities, organizations, or individuals.
2. Second, the volume and size of digital evidence may be massive and may often require complex processing, using methods such as big data analytics or digital forensics, in order to be readable and subsequently used as evidence in court. Although the actual volume of data to be used in court may not necessarily be as large as compared to other types of documentary evidence, the processing of the raw dataset generated by, for instance, Facebook, WhatsApp, or telecom interceptions, will often require the use of specific technical tools to manage, analyse, and filter the relevant data.[20]
3. Third, forensic science will often be required in order to trace the original source of the digital evidence, as well as to classify and verify its content. Accordingly, digital evidence should not be readily admissible in court and should instead be tendered via witness examination or via expert report. This will necessarily entail that digital evidence, regardless of its

[15]Ibid.

[16]Civil society organizations play an important role in the performance of fact-finding activities, including the gathering of evidence for the purposes of prosecuting individuals before national or international jurisdictions. Some of these organizations have focused on the use of open-source data to investigate human rights abuses and the commission of international crimes. This methodology is known as open-source intelligence (OSINT). Organizations such as Human Rights Watch or Bellingcat use publicly available data and evidence reported by ordinary citizens to cross-examine it and drawing conclusions, in order to document the events taking place in conflict zones.

[17]See Leiden Guidelines, *supra* note 9, at 20, 29.

[18]K. Aksamitowska, 'Digital Evidence in Domestic Core International Crimes Prosecutions: Lessons Learned from Germany, Sweden, Finland and The Netherlands', (2021) 19 *Journal of International Criminal Justice* 189, at 192–3.

[19]See, for instance, the implications of the US Court ordering Facebook to disclose posts that had been previously deleted from the platform in order to seek evidence relating to anti-Rohingya hate speech and incitement to violence, so that they might potentially be used before the International Court of Justice as evidence of Myanmar's alleged responsibility for genocide. A. Koenig, 'Q&A on Court Ordering Facebook to Disclose Content on Myanmar Genocide', *Just Security and Tech Policy Press*, 24 September 2021, available at www.justsecurity.org/78358/qa-on-court-ordering-facebook-to-disclose-content-on-myanmar-genocide/.

[20]T. Hussain Sheikch and R. Gupta, 'Big Data Analysis and Digital Forensic', (2018) 4(2) *International Journal of Scientific and Technical Advancements* 207, at 209.

https://doi.org/10.1017/S0922156523000031 Published online by Cambridge University Press

provenance, should be reasonably supported by either forensic science and/or witness statements in order to be reliable and effectively used in the courtroom.[21]

It follows that digital evidence may often undergo processes that are not traditionally used for other types of physical evidence. This might in turn require investigators to ensure adequate preservation of digital evidence, while demanding international courts and tribunals to use a different – and often, higher – threshold for the admissibility and examination of digital evidence in the courtroom, as will be further developed in Section 3.2.

2.2 The impact of digital evidence on international criminal investigations

Documentation and fact-finding activities on the ground, before competent investigative authorities engage in the investigation, have proved extremely useful to ensure access to information, thus promoting accountability efforts in conflict situations.[22]

The need to act promptly, before any potential criminal evidence is taken or destroyed, is essential to avoid accountability gaps. Civil society organizations carry out invaluable work on the ground to identify and locate victims and potential witnesses, to map victimization, and to collect any relevant information on both the victims and the alleged perpetrators.[23] This information must be adequately preserved in order to pass it to the competent investigative authorities.

Digital footprint may unknowingly leave traces of the perpetration of crimes, and thus these records may become critical for establishing evidentiary connections to international crimes.[24] While physical documentary records may be easily destroyed by perpetrators before any investigators get to the ground, digital data, e.g., call records, bank statements, emails, or internet search history, are presumably harder to lose trace of, since they are hosted in data processing centres located far away from the conflict area. Therefore, if adequately collected, preserved, and verified, digital records may serve as direct evidence – or, at least, powerful indicators – for the establishment of criminal patterns.[25]

Today, the democratization of public speech through social media platforms, together with the capacity of civil society to engage in the investigation of mass atrocities, can also be helpful for investigators for several reasons. First, social media may help tracking where the relevant physical evidence and potential witnesses may be located. Second, it can be used to map the relevant zones where the crimes may have taken place. Third, they may provide relevant information for establishing patterns that may ultimately prove useful at trial for the assessment of the elements of the crimes.[26]

As useful and traceable as digital data might be for the purposes of identifying and tracking criminal patterns, digital evidence might also prove deceiving and unreliable – particularly, when it comes to open-source evidentiary materials. Authors such as Koenig, Irving, McDermott, or Murray have thoroughly discussed the inherent biases of open-source evidence,[27] and the key principles that should guide the production of digital, open-source, evidence in international

[21]D. B. Garrie and J. D. Morrissy, 'Digital Forensic Evidence in the Courtroom: Understanding Content and Quality', (2014) 12(2) *Northwestern Journal of Technology and Intellectual Property* 122, at 125–7.

[22]Eurojust, 'Documenting International Crimes and Human Rights Violations for Accountability Purposes: Guidelines for Civil Society Organisations', *Eurojust*, 21 September 2022, at 5, available at www.eurojust.europa.eu/publication/documenting-international-crimes-and-human-rights-violations.

[23]Ibid., at 16.

[24]See, e.g., the relevant case law examples provided by Freeman, *supra* note 4, at 307 et seq.

[25]J. Paladino, 'Can a Tweet be Evidence? How Social Media is Being Used to Hunt Down War Crimes in Ukraine', *GRID*, 11 April 2022, available at www.grid.news/story/global/2022/04/11/in-ukraine-war-crimes-are-being-captured-on-social-media/.

[26]Ibid.

[27]See, e.g., Y. McDermott, A. Koenig and D. Murray, 'Open Source Information's Blind Spot: Human and Machine Bias in International Criminal Investigations', (2021) 19(1) *Journal of International Criminal Justice* 85.

https://doi.org/10.1017/S0922156523000031 Published online by Cambridge University Press

criminal proceedings.[28] The need to have uniform standards when dealing with digitally-derived evidence has also been addressed by the Berkeley Protocol and the Leiden Guidelines. The remainder of this article will, on its part, be devoted on how both the prosecution and the defence may make use of such digital evidentiary sources, and how these advantages may impact the equality of arms principle in proceedings before the ICC.

3. The challenges brought by digital evidence in the conduction of a fair trial: A discussion from the perspective of the equality of arms principle

The challenges that the collection, preservation, analysis, and assessment of digital evidence may bring about will be examined in the following sections from a fair trial rights perspective. Accordingly, Section 3.1 will provide a general overview of the main provisions set out in the Rome Statute of the International Criminal Court (the Rome Statute) to ensure equality of arms between the parties, while Section 3.2 will discuss how these safeguards may be altered by the introduction of digital evidence in criminal proceedings before the ICC.

3.1 General safeguards provided under the ICC framework as regards the gathering and use of evidence in court to guarantee equality of arms

Respect for the equality of arms principle is imperative in order to ensure the legitimacy of criminal proceedings.[29] Both civil and common law systems envisage this right as an inherent element of a fair trial. Accordingly, parties to a criminal dispute must be afforded with reasonable opportunities to present their case under equal procedural conditions.[30] The applicability of the principle of equality of arms has also been recognized in the conduct of international criminal proceedings.[31]

Article 67 of the Rome Statute enshrines minimum safeguards to ensure compliance with the equality of arms principle throughout the proceedings, including the right of the accused to have adequate time and resources for the preparation of the case, to be granted with legal assistance, to submit its own evidence and examine the opposing party's witnesses under the same conditions as the prosecution, and to have disclosed evidence in possession of the Office of the Prosecutor (OTP) which may somehow prove material for the defence strategy.[32]

The *raison d'être* of these guarantees is the asymmetrical relationship the parties find themselves in from the very beginning of an investigation of a given situation. As previously mentioned, civil society may be involved in the investigation of human rights violations even before a situation is referred to the ICC or opened with the Chambers' authorization.[33] These preliminary

[28]See, e.g., A. Koenig et al., 'New Technologies and the Investigation of International Crimes: An Introduction', (2021) 19 *Journal of International Criminal Justice* 1.

[29]International standards consider the right to a fair trial as an imperative principle in criminal proceedings. See, *inter alia*, Universal Declaration of Human Rights, UNGA Res. 217A(III), UN Doc. A/810 (1948), Arts. 10–11; 1966 International Covenant on Civil and Political Rights, 999 UNTS 171 (1966), Art. 14; 1950 European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols No. 11 and No. 14, ETS 5 (1950), Art. 6; 1969 American Convention on Human Rights, 1144 UNTS 123 (1969), Art. 8; 1981 African Charter on Human and Peoples' Rights, 1520 UNTS 217 (1981), Art. 7.

[30]S. Negri, 'Equality of Arms – Guiding Light or Empty Shell?', in M. Bohlander (ed.) *International Criminal Justice: A Critical Analysis of Institutions and Procedures* (2007), 13, at 15.

[31]In the *Tadić* decision, the Appeals Chamber of the International Criminal Tribunal for the Former Yugoslavia stated that 'the principle of equality of arms must be given a more liberal interpretation than that normally upheld with regard to proceedings before domestic courts'. See *The Prosecutor v. Duško Tadić* (Judgement), IT-94-1-A, 15 July 1999, paras. 52–55. Further discussion on the equality of arms principle from the perspective of human rights law may be found in W. Schabas, *The International Criminal Court: A Commentary on the Rome Statute* (2016), 1024–5.

[32]1998 Rome Statute of the International Criminal Court 2187 UNTS 90 (1998), Art. 67 (Rome Statute).

[33]See Section 2.2, *supra*.

https://doi.org/10.1017/S0922156523000031 Published online by Cambridge University Press

fact-finding activities may ultimately help the OTP once the investigation is open.[34] After that, the OTP relies on specialized investigation teams to gather and examine the evidence on the ground.[35] Additionally, the OTP may request co-operation and assistance from states and international organizations to ensure the effectiveness of the evidence gathering process.[36] Consequently, the OTP usually benefits from a more lengthy and specialized investigation than the defence does.

Defence teams start investigating the case with significantly less information, time, and resources as compared to the OTP.[37] While it is certain that the prosecution bears the burden of proof through the entire course of the proceedings,[38] and thus must be afforded with sufficient resources to lead the investigation, the threshold for defence teams to challenge the prosecution's case may be at times too high.

The Rome Statute provides for certain rights and duties which aim at bridging the gap between the prosecution and the defence when adducing evidence in court. The following ones are essential in order to balance the parties' opportunities as regards the gathering of evidence:

1. Article 54(1) of the Rome Statute acknowledges the OTP's duty to investigate both incriminating and exonerating circumstances equally.
2. Article 67(2) of the Rome Statute embeds the prosecutorial duty to disclose to the defence evidence in the prosecution's possession that is material to the preparation of the defence. However, the OTP may refuse to disclose evidence that is either restricted due to confidentiality reasons,[39] or based on national security grounds.[40] Also, the OTP may withhold certain evidence from disclosure if it may endanger the safety of witnesses or their families, and submit a summary of the information instead.[41]
3. Articles 61(3) and 64(3)(c) of the Rome Statute establish the Chambers' duty to disclose the evidence upon which the OTP will rely before the confirmation of charges hearing[42] and trial hearing.[43]

Besides the Rome Statute, the ICC Rules of Procedure and Evidence develop the rules on disclosure for both the OTP and the defence to safeguard equality of arms. Accordingly, documents and information in the possession of the prosecution which are material to the preparation of the defence, or which are intended for use by the Prosecutor as evidence, must be disclosed to the defence in advance to enable adequate preparation.[44] However, Rules 81 and 82 provide for certain restrictions to the duty of disclosure. Some of these limitations concern the likelihood of potential prejudice to the conduction of further or ongoing investigations, in which case the Chambers may decide whether that information may be withheld.[45] On the other hand, the defence must provide

[34]For instance, in the Darfur situation, the OTP used satellite images generated by the Satellite Sentinel Project to further its investigation into Abdel Raheem Muhammad Hussein, who was issued an arrest warrant in 2012 that has not yet been successfully enforced. Most of these documents and records remain restricted due to confidentiality reasons. The Satellite Sentinel Project was conceived to produce analysis reports on satellite imagery and data patterns, for the purposes of monitoring potential hotspots and threats to human security. See 'Satellite Sentinel Project', available at www.enoughproject.org/about/past-campaigns/satellite-sentinel-project.

[35]See Regulations of the Office of the Prosecutor, ICC-BD/05-01-09, 23 April 2009, Regulation 8.

[36]See Rome Statute, *supra* note 32, Art. 87.

[37]Office of the Prosecutor, *Policy Paper on Preliminary Examinations* (2013), para. 2 (OTP Policy Paper 2013).

[38]See Rome Statute, *supra* note 32, Arts. 54, 67.

[39]Ibid., Art. 54(3)(e).

[40]Ibid., Art. 72.

[41]Ibid., Art. 68(5).

[42]Ibid., Art. 61(3).

[43]Ibid., Art. 64(3)(c).

[44]International Criminal Court Rules of Procedure and Evidence, ICC-PIOS-LT-03-004/19_Eng (2019), Rule 77 (Rules of Procedure and Evidence).

[45]Ibid., Rule 81(2).

https://doi.org/10.1017/S0922156523000031 Published online by Cambridge University Press

the OTP with the evidence on which the accused intends to rely on when raising a ground for the exclusion of criminal responsibility.[46]

In terms of evidence gathering in the course of ICC proceedings, the OTP is usually ahead of the defence at the initial stages of the criminal investigation, as already stated, which makes disclosure essential for the defence to keep up with the information gathered by the prosecution that may be relevant for the defence. The design of the initial reactive defence strategy, which aims at challenging the prosecution's preliminary findings regarding the facts involving the suspect and the possible counts they will be charged with, will only be effectively developed once full disclosure of the evidence is made.[47]

The ICC Chambers Practice Manual provides that the Prosecutor has the duty to disclose to the defence all evidence in their possession or control that 'may show the innocence of the person, or mitigate the guilt of the person or may affect the credibility of the prosecution evidence', as soon as practicable – ideally, before the confirmation hearing takes place – and on a continuous basis.[48] This may include both incriminating and exonerating materials. The ICC Chambers have adopted differing views as to what extent incriminating materials might be relevant for the defence in order for the prosecution to fulfil its disclosure duty. In many instances, the Chambers indicated the Prosecutor to provide a summary table or chart, along with the evidentiary materials, that points to the relevant information that has been disclosed.[49] However, such an obligation cannot be imposed on the Prosecutor, who may not disclose internal documents, reports, or memoranda prepared by the OTP.[50]

The latter point, i.e., to what extent the prosecution may disclose not only the original materials, but also the methodology used for their examination, becomes particularly relevant when it comes to the use of digital sources of evidence. The defence needs to know and test the evidence collected by the counterpart in order to be able to react to it. When it comes to digital evidence, the evidence that is ultimately used is usually just a small part of all the raw information that the prosecution had accessed to, after having filtered and selected it. For instance, if the prosecution intends to adduce a report describing certain call records and the IP addresses from where these calls took place, and the defence did not participate in the selection of the relevant data, defence counsels would not only need to access all other call records in order to be able to show the irrelevance of the presented data.[51] They must also be able to test the methodology used by the OTP in order to contrast their findings.

While the aforementioned provisions from both the Rome Statute and the Rules of Procedure and Evidence aim at alleviating the late start of the investigation by the defence, in practice, it is dubious whether equal efforts are invested by the OTP in order to investigate potentially exonerating and incriminating circumstances alike.[52] Furthermore, defence teams often suffer from a delayed disclosure of the evidence, whilst experiencing serious hurdles when conducting their own investigation.[53]

The following sections will draw on the particular challenges that the introduction of digital evidence may pose for balancing fair trial rights in ICC proceedings.

[46]Ibid., Rule 79.

[47]C. Buisman and D. Hooper, 'Defense Investigations and the Collection of Evidence', in C. Rohan and G. Zyberi (eds.), *Defense Perspectives on International Criminal Justice* (2017), 519, at 520.

[48]International Criminal Court Chambers Practice Manual (2021), para. 21.

[49]*Prosecutor v. Bosco Ntaganda*, Decision Setting the Regime for Evidence Disclosure and Other Related Matters, ICC-01/04-02/06-47, 12 April 2013, para. 32.

[50]See Rules of Procedure and Evidence, *supra* note 44, Rule 81(1). See also X. J. Keïta, 'Disclosure of Evidence in the Law and Practice of the ICC', (2016) 16 *International Criminal Law Review* 1018, at 1035.

[51]M. Simonato, 'Defence Rights and the Use of Information Technology in Criminal Procedure', (2014) 85(1) *Revue international de droit pénal* 261, at 287.

[52]C. Buisman, 'The Prosecutor's Obligation to Investigate Incriminating and Exonerating Circumstances Equally: Illusion or Reality?', (2014) 27 *Leiden Journal of International Law* 205, at 211.

[53]See Buisman and Hooper, *supra* note 47, at 558.

https://doi.org/10.1017/S0922156523000031 Published online by Cambridge University Press

3.2 The collection, preservation, analysis, admissibility, and assessment of digital evidence in ICC proceedings: Main challenges in the achievement of equality of arms

The collection, preservation, and verification process of digital evidence is a particularly resource-intensive task.[54] Digital evidence requires both hardware and software in order to be readable, which often poses technical challenges on the experts, lawyers and judges interpreting this data.[55] The parties to the ICC proceedings may not be adequately equipped with the necessary resources, expertise, and institutional backup that the procurement of digital evidence demands.

Given the difficulties that the digital environment entails, the following sections will examine whether these obstacles may lead to unequal opportunities between the parties throughout the following stages: access and collection of the evidence (Section 3.2.1); analysis of its reliability (Section 3.2.2); and admissibility and assessment of digital evidence (Section 3.2.3).

3.2.1 Access to and collection of sources of digital evidence

An adequate collection and preservation of all the materials to be used for the production of pieces of evidence is paramount in order to avoid them being rendered inadmissible in court. The collection of digital media refers to the access to the 'raw materials' to be analysed, e.g., hard drives, mobile phones, optical media, storage digital cards, and document files drawn from databases, *inter alia*.[56] These items must be stored and preserved in compliance with forensic standards, including the chain of custody, so as to ensure their veracity and traceability.[57]

The increasing reliance on publicly available digital information and the use of IT technologies for analysing it has democratized access to raw data by either party to the proceedings. As already mentioned, the OTP counts on a wide range of resources to collect evidence on the ground,[58] while the defence may often have access to privileged information from the accused, which allows them to focus their search for exonerating circumstances.[59] The following subsections will examine how each of the parties to the proceedings may deal with issues relating to the collection of digital evidentiary material.

3.2.1.1 The challenges in the collection of digital evidence faced by the OTP. The Prosecution, which bears the burden of proof throughout the criminal proceedings, must be allocated with sufficient resources to be able to determine: first, whether there is a 'reasonable basis' to conduct a full examination on a given situation and to point to certain suspects before a case is open at the ICC;[60] and second, to prove in trial 'beyond reasonable doubt' whether the alleged charges have been perpetrated by the defendant.[61]

In pursuit of the material truth, the OTP shall 'investigate incriminating and exonerating circumstances equally' under Article 54(1)(a) of the Rome Statute. This is in line with the position it holds throughout the proceedings and the institutional backup it receives from the ICC, for it is considered that the OTP is conveniently positioned to gather information at the earliest possible stage, i.e., during preliminary examinations.[62]

[54]See Freeman, *supra* note 4, at 329–33.

[55]See Mehandru and Koenig, *supra* note 13.

[56]C. Altheide and H. Carvey, *Digital Forensics with Open Source Tools* (2011), 3.

[57]See HRC Report 2018, *supra* note 14, at 9.

[58]See Section 2.2, *supra*.

[59]See, e.g., the submissions presented by the defence in the case of *The Prosecutor v. Jean-Pierre Bemba Gombo, Aimé Kilolo Musamba, Jean-Jacques Mangenda Kabongo, Fidèle Babala Wandu and Narcisse Árido,* Narcisse Arido's response to Bemba and Kilolo's Requests for an *Ex Parte* Defence Only Status Conference to Discuss Privileged Materials, ICC-01/05-01/13, 12 May 2015, paras. 4–6.

[60]See Rome Statute, *supra* note 32, Art. 15(1).

[61]Ibid., Art. 66(3).

[62]Koenig et al., 'Open Source Fact-Finding in Preliminary Examinations', in M. Bergsmo and C. Stahn (eds.), *Quality Control in Preliminary Examination: Volume 2* (2018), 681, at 681–2.

https://doi.org/10.1017/S0922156523000031 Published online by Cambridge University Press

Until recently, the collection and use of these materials was highly centralized and institutionalized. Today, personal data relating to telecommunications, geolocation or imagery is scattered among various public entities, business companies and private individuals alike, or it might well be readily available on the internet. Although the OTP invests in expertise from cyber-investigators and analysts to build internal evidence-gathering capacity,[63] it is increasingly relying on strategic partnerships with private entities, civil society, and other bodies which engage in digital fact-finding activities.[64]

However, an overreliance on external partners to gather digital materials may lead to certain inconsistencies or difficulties for the prosecution during the pre-trial phase or when building up the potential evidence to be used in the courtroom:

1. First, external partners do not abide by mandatory standards in terms of collection and preservation of information and gathered materials as the OTP does. While the OTP has the duty to investigate both incriminating and exonerating circumstances, civil society organizations or private entities do not have such a duty.[65] Therefore, the collection of digital evidence relying on partners outside the ICC institution may interfere with the OTP's fulfilment of its duty to look for both incriminating and exculpatory circumstances.
2. Second, an oversupply of information – in addition to the inherently voluminous nature of digital data – may lead to higher constraints for the prosecution when filtering and discerning relevant materials. This may turn investigations into a highly demanding process in terms of resources, time, and expertise, in order to ensure that the evidence collected is reliable, verifiable, and traceable.[66]
3. Third, the prosecution may encounter serious difficulties to establish the probative value of digital evidence, particularly, of open-source information. In a world with increasingly deceiving information and deepfakes, providing a clear chain of custody is key to establish *prima facie* authenticity.[67] If external information providers have not adequately preserved the evidence collected, the digital evidence's probative value may be undermined.

Consequently, a major challenge for the OTP when collecting evidence during criminal investigations is to ensure the reliability of the sources of information and the authenticity of the materials collected. The fact that the OTP may co-operate with external information providers for evidence gathering purposes does not necessarily mean that the prosecution will be able to introduce these materials in the courtroom. Conversely, the OTP will most likely face difficulties for establishing the reliable provenance of those materials, and thus will require a great deal of resources and time.

Guidelines on the practice and use of digital evidence in international criminal proceedings – e.g., the Leiden Guidelines or the Berkeley Protocol – aim at harmonizing the standards for the treatment of digitally-derived evidence, including their treatment during criminal investigations. The use of uniform standards by both civil society organizations working on the ground and the

[63]Office of the Prosecutor, *Strategic Plan 2016-2018*, Policy Paper (2015), para. 63.

[64]E. McPherson, I. Guenette Thornton and M. Mahmoudi, 'Open Source Investigations and the Technology-Driven Knowledge Controversy in Human Rights Fact-Finding', in S. Dubberley, A. Koenig and D. Murray (eds.), *Digital Witness: Using Open Source Information for Human Rights Investigation, Documentation, and Accountability* (2020), 68, at 71–2.

[65]For this reason, the ICC Prosecutor, Kharim Khan, and Eurojust, have launched practical guidelines for documenting and preserving information on international crimes, addressed to civil society organizations. See Eurojust, *supra* note 22.

[66]See Freeman, *supra* note 4, at 333.

[67]E. Irving, R. Heinsch and S. Rewald, 'Using the Leiden Guidelines to Address Key Issues in Digitally Derived Evidence', *OpinioJuris*, 23 August 2022, available at www.opiniojuris.org/2022/08/23/using-the-leiden-guidelines-to-address-key-issues-in-digitally-derived-evidence/.

https://doi.org/10.1017/S0922156523000031 Published online by Cambridge University Press

OTP investigation teams may certainly mitigate problems relating to the methods of collection and preservation of the evidence at the initial stages of investigations.

3.2.1.2 The challenges in the collection of digital evidence faced by the defence. From the moment the OTP points out to a certain suspect, and particularly during the pre-trial stage, defence teams need to know: (i) first, what evidence the counterpart has collected, in order to be able to challenge its admissibility and probative value; and (ii) second, what new evidence the defence may bring to the table for the purposes of building up an alternative theory of the case.

Consistently, defence teams count on two main sources of information: on the one hand, evidence that has been collected by the OTP and that is disclosed to the defence, and, on the other hand, evidence that may be directly obtained from the accused. Certainly, defence counsels may often have access to privileged information from the accused, who may point them to helpful sources of evidence, thereby narrowing the scope in the search for exonerating materials.[68]

The defence may sometimes try to use their own research capacity to gain access to evidentiary material. For instance, in the *Ayyash et al.* case before the STL, the Badreddine and Oneissi defence counsels proceeded to collect their own open-source evidentiary material, namely WikiLeaks documents.[69] However, these were ultimately deemed inaccurate and unverifiable by the STL Trial Chamber, thus rendering them inadmissible.[70]

In practice, when approaching potential sources of evidence, defence teams may face considerable budgetary and resource constraints,[71] while experiencing more difficulties to turn to external support as compared to the OTP. The defence does not have an easy access to external partnerships as the prosecution does.[72] Accordingly, defence teams may struggle to collect suitable exonerating materials on their own motion to build a robust defence strategy.

Moreover, the accused also counts on the evidence disclosed by the prosecution that is material to their defence strategy, either because it contains exonerating materials or because the Prosecutor intends to rely on the collected incriminating evidence at trial. In that case, defence teams will aim to challenge the authenticity, reliability, and probative value of the incriminating evidence disclosed by the prosecution. While, in principle, the OTP is in charge of scrutinizing the reliability of any information at its disposal,[73] the defence may want to test the validity of the evidence. In other words, the defence may want to verify the adequacy of the methodology used by the OTP's experts to see whether forensic standards were fully respected and whether the relevant data was selected in an unbiased manner.[74]

For that purpose, defence teams should get access, not only to the 'raw material' or the database that constitutes the source of the evidence, but also to the methodology used by the prosecution for the analysis, selection, and interpretation of the original data. That would allow the defence to cross-check any possible evaluation inconsistencies during the whole analytical process.

The foregoing reveals the importance of full and timely disclosure of all this information to the counterpart when it comes to digital evidence. A full understanding of the data collected by the prosecution cannot be achieved without understanding their nature and the scientific methods used for their selection. Otherwise, defence teams may find themselves with large amounts of data

[68]See, e.g., the submissions presented by the defence in the case of *The Prosecutor v. Jean-Pierre Bemba Gombo, Aimé Kilolo Musamba, Jean-Jacques Mangenda Kabongo, Fidèle Babala Wandu and Narcisse Árido*, Narcisse Arido's response to Bemba and Kilolo's Requests for an *Ex Parte* Defence Only Status Conference to Discuss Privileged Materials, ICC-01/05-01/13, 12 May 2015, paras. 4–6.

[69]*The Prosecutor v. Salim Jamil Ayyash et al.*, Decision on the Admissibility of Documents Published on the WikiLeaks Website, STL-11-01/T/TC, 21 May 2015.

[70]Ibid., paras. 40–43.

[71]See Section 3.2.2, *infra*.

[72]See Buisman and Hooper, *supra* note 47, at 539.

[73]See OTP Policy Paper 2013, *supra* note 37, para. 27.

[74]D. Jacobs, 'Methodological Challenges Relating to the Use of Third-Party Human Rights Fact-Finding in Preliminary Examinations', *Article 15 Communication*, 27 May 2019, para. 88.

https://doi.org/10.1017/S0922156523000031 Published online by Cambridge University Press

to be examined that have already been curated by the OTP's experts, without guidance on how to approach such data, and with little time and resources to find out how they selected them.

However, a consistent practice on disclosure matters is still lacking in the context of ICC proceedings,[75] which makes it difficult for defence teams to effectively challenge the prosecution's evidence due to time constraints, lack of resources, and lack of information.

3.2.2 The analysis of digital evidence: Reliability, authenticity, and interpretation of the evidence

Digital material poses new challenges in terms of identification and verification of their content.[76] Once collected and stored, digital data will undergo a curation process, in order to understand the meaning and relevance of the raw data. For instance, it is likely that data may be subject to decryption or statistical analysis and be further interpreted by forensic experts.[77]

For both parties to the proceedings, it is not only essential to count on adequate resources to process such raw data, but also to disclose it to each other in an intelligible format, while sharing the methodology with the counterpart – and, at a later stage, with the judges – in an understandable and transparent manner.[78] The challenges that both the OTP and the defence may face when dealing with the analysis of the digital evidence collected will be further developed below.

3.2.2.1 The challenges in the analysis of digital evidence faced by the OTP. The Prosecution bears the burden of proof to show, beyond reasonable doubt, that the alleged perpetrator is responsible for the charges pursued against him or her. For that reason, when dealing with pieces of digital evidence, the OTP must ensure that the selected data that the prosecution intends to use as evidence in court has been adequately verified by forensic experts, and that the interpretation given follows a sound scientific method.

In terms of authenticity and verification of the data, in a world with increasing concern on misinformation and deepfakes, there is a risk that digital evidence used at trial may have been manipulated.[79] Not only the content itself may have been tampered, but also the metadata informing about the time, place and authorship of the digital material might be deceiving.

In the *Bemba et al.* case, the defence challenged the screenshots of photographs posted on Facebook which were introduced as evidence by the prosecution, on the grounds of lack of forensic verification of the metadata.[80] In its final judgment, however, the Trial Chamber did not address their admissibility, as it considered that the facts were sufficiently proved by other means of evidence, and thus the screenshots were not directly relevant to the *ratio decidendi*.[81]

Situations such as the foregoing call for the allocation of sophisticated technological methods and clear guidelines to guarantee the authenticity of the footage presented as evidence, as well as adequate training of the forensic experts that carry out the verification process.[82]

Furthermore, digital materials will most likely need to go through an interpretative process in order to be presented as evidence. The implications of digital evidence on the material object of the criminal proceedings may sometimes only be inferred once the digital material has undergone an analysis made by expert reports.

[75]See Section 3.1, *supra*. See also IBA Report, *supra* note 10, at 37.

[76]See Koenig et al., *supra* note 62, at 700.

[77]See Altheide and Carvey, *supra* note 56, at 4.

[78]See IBA Report, *supra* note 10, at 23.

[79]L. Freeman, 'Prosecuting Atrocity Crimes with Open Source Evidence: Lessons from the International Criminal Court', in Dubberley, Koenig and Murray, *supra* note 64, at 65. See also C. Koettl, D. Murray and S. Dubberley, 'Open Source Investigation for Human Rights Reporting: A Brief History', in ibid., at 21.

[80]*The Prosecutor v. Jean-Pierre Bemba Gombo et al.*, 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, 9 October 2015, paras. 83–86.

[81]See Freeman, *supra* note 4, at 328.

[82]See IBA Report, *supra* note 10, at 26.

https://doi.org/10.1017/S0922156523000031 Published online by Cambridge University Press

The prosecution may face serious challenges when trying to present the digital evidence in a transparent and understandable format to the counterpart and to the bench. The selection of data originating from certain self-learning AI-empowered systems, which entirely rely on algorithms, may be at times difficult to track, and thus to interpret. It is yet to be seen how both the prosecution and the Chambers will deal with these issues, in light of the increasing reliance on social media imagery as source of evidence.[83]

3.2.2.2 The challenges in the analysis of digital evidence faced by the defence. In their analysis of the incriminating evidence disclosed by the prosecution, the defence will only need to raise doubt about the reliability of the materials presented in trial, in view of the standard of proof afforded in international criminal proceedings. However, providing a counter-report to challenge the OTP's evidence may be particularly burdensome and challenging for defence teams. Defence teams will need to build up an alternative methodology to assess the evidence with less time, information, and resources than the prosecution counts on.

By way of example of the resources allocated to defence teams, most of the alleged perpetrators of crimes under investigation at the ICC are provided with legal aid[84] and will be represented by an independent defence team that must be created from scratch.[85] The Office of Public Counsel for the Defence may grant administrative and legal assistance to the defendants, especially while pending the appointment of a defence team.[86] Yet, the Assembly of States Parties has acknowledged that the legal aid scheme is insufficient. For the year 2022, it proposed to raise the budget for defence counsels by 40 per cent, amounting to approximately €5,573,000 in total, based on the assumption that 11 defence teams are financed by legal aid,[87] and according to the regulations set out in the ICC Legal Aid Policy.[88] Yet, a report issued by the Group of Independent Experts to the Assembly of States Parties suggested a revision of the legal aid scheme.[89] On top of the budgetary constraints, defence teams face a lack of adequate working spaces,[90] and a lack of institutional backup when pursuing co-operation with states or organizations.[91]

The foregoing picture is only an illustration of the conditions defence counsels deal with when confronting an accusation that has been ahead of the investigation for years. Defence teams would benefit from cross-examining the reliability of the evidence presented by the OTP with the help of party-appointed experts. However, the few resources they count on may prevent them from resorting to forensic analyses at all, thus being left with no alternatives than relying entirely on the OTP's own examination on the provenance and the authenticity of the digital evidence presented.

Overall, and considering the nature and volume of digital evidence, as well as the expertise required to challenge its content, this is likely to put the defence in a disadvantageous position from a very early stage of the proceedings. In order to alleviate such burdens, the accused should be fully informed about the methodology followed by the prosecution to infer the intended

[83]See, e.g., the evidence adduced for the purposes of issuing the arrest warrant in *The Prosecutor v. Mahmoud Mustafa Busayf Al-Werfalli*, Second Warrant of Arrest, ICC-01/11-01/17, 4 July 2018, para. 19.

[84]Assembly of States Parties, Report on the Performance of the Court's Legal Aid System in 2017, ICC-ASP/17/3 (3 May 2018), at 2.

[85]See Buisman and Hooper, *supra* note 47, at 521.

[86]Regulation 77 of the Regulations of the Court, ICC-BD/01-05-16 (as amended on 12 November 2018).

[87]Assembly of States Parties, Proposed Programme Budget for 2022 of the International Criminal Court, ICC-ASP/20/10 (16 August 2021), at 121 and Ann. II.

[88]Assembly of States Parties, Registry's Single Policy Document on the Court's Legal Aid System, ICC-ASP/12/3 (4 June 2013).

[89]Assembly of States Parties, Report of the Bureau on Legal Aid, ICC-ASP/20/39 (1 December 2021), at 4–5.

[90]M. Fedorova, 'The Principle of Equality of Arms in International Criminal Proceedings', in C. Rohan and G. Zyberi (eds.), *Defense Perspectives on International Criminal Justice* (2017), 204, at 219.

[91]See Buisman and Hooper, *supra* note 47, at 539.

https://doi.org/10.1017/S0922156523000031 Published online by Cambridge University Press

consequences at trial, in order to adequately verify the source and provide a counter-report, as well as to procure access to forensic tools that may help defence teams in the examination process.

3.2.3 Admissibility and assessment of evidence at trial

If the evidence submitted was challenged by either party, the ICC bench must analyse the *prima facie* authenticity and reliability of the evidence, along with verifying the accuracy of the selection process of the sources of data, in order to admit the evidence and assess its probative value at trial.[92]

The inherent complexity of digital evidence and its voluminous nature would require a nuanced assessment of its authenticity and its relevance for the object of the proceedings. Considering the risk of forgery and the high burden that parties will likely bear to challenge the reliability and probative value of digital evidence, the ICC rules on admissibility and assessment of evidence should be strictly applied to ensure the integrity of the criminal proceedings. This section aims at providing a re-examination of the rules on admissibility of the evidence and the assessment of its probative value.

3.2.3.1 Admissibility of digital evidence. The Rome Statute leaves the ICC Chambers with broad discretion when deciding on the admissibility of the evidence submitted by the parties. Article 69(4) of the Rome Statute, as interpreted by the Court, provides that the admission of any tendered material needs to satisfy a three-part test: (i) it must be relevant to the case; (ii) it must have probative value; and (iii) its probative value must outweigh any prejudicial effect that might be caused by its admission.[93]

The Chambers may assess the probative value of the evidence presented based on various factors, including its reliability and authority.[94] The third element of the admissibility test refers to any prejudice that the admission of a given piece of evidence might cause to the fair conduction of the proceedings.[95] Nonetheless, this does not mean that prejudicial evidence will be automatically excluded from assessment at trial. Rather, the Chambers will decide to exclude it only if its potential prejudicial effect outweighs its probative value.[96]

Furthermore, Article 69(7) envisages two grounds for the exclusion of evidence, if: (i) the evidence is unreliable; or (ii) its admission would be antithetical. The latter would include evidence that has been collected in violation of internationally recognized human rights, although, so far, the ICC's case law has only raised concerns in this regard on the admission of evidence that contravenes the right to privacy or 'private life'.[97]

The ICC Chambers also enjoy discretion as to when to rule on the admissibility of evidence, since the Chambers Directions on the conduct of proceedings recognize the possibility of parties to submit items of evidence 'without a prior ruling on relevance and/or admissibility'.[98] Accordingly, the Chambers may either issue a prompt ruling on admissibility, or wait instead until

[92]*The Prosecutor v. Jean-Pierre Bemba Gombo*, Decision on the Prosecution's Application for Admission of Materials into Evidence Pursuant to Article 64(9) of the Rome Statute, ICC-01/05-01/08, 8 October 2012, para. 9; *The Prosecutor v. Germain Katanga and Mathieu Ngudjolo Chui* (Decision on the Prosecutor's Bar Table Motions), ICC-01/04-01/07, 17 December 2010, para. 24.

[93]*The Prosecutor v. Jean-Pierre Bemba Gombo*, Decision on the Prosecution's Application for Admission of Materials into Evidence Pursuant to Article 64(9) of the Rome Statute, ICC-01/05-01/08, 8 October 2012, para. 7.

[94]Ibid., para. 8.

[95]Ibid.

[96]Ibid.

[97]*The Prosecutor v. Mr Jean-Pierre Bemba Gombo, Mr Aimé Kilolo Musamba, Mr Jean-Jacques Mangenda Kabongo, Mr Fidèle Babala and Mr Narcisse Arido*, Appeals Chamber Judgment Pursuant to Article 74 of the Statute, ICC-01/05-01/13-2275-Red, 8 March 2018, para. 371. See also Freeman, *supra* note 4, at 294–5.

[98]*The Prosecutor v. Al Hassan*, Second Decision on the Introduction of Prior Recorded Testimonies Pursuant to Rule 68(3) of the Rules, ICC-01/12-01/18-1267-Red, 26 January 2021, para. 24.

https://doi.org/10.1017/S0922156523000031 Published online by Cambridge University Press

the issuance of the final judgment.[99] Usually, the Chambers opt for the latter, for the purposes of considering the 'relevance and probative value as part of the holistic assessment of all evidence submitted when deciding on the guilt or innocence of the accused'.[100] That being the case, the parties would not know whether their evidence has been admitted until the very end of the proceedings,[101] thus having to deal in trial with the examination of every single item submitted as evidence.

The matter of how and when to rule on the admissibility of evidence becomes particularly relevant when the parties tender highly voluminous and complex items of evidence, as digital materials are. In those cases, the preparation of their introduction in court (via experts or witness testimonies) and their cross-examination may be a resource-intensive task, thus affecting the equality of arms.

Despite the substantive complexity of ICC proceedings and the high volume of evidence presented in court, the Chambers have traditionally been particularly lenient when applying the rules on admissibility.[102] In recent years, the Chambers have ruled on the early exclusion evidence only on a few occasions. For instance, in *Bemba et al.*, the Trial Chamber decided to rule early on the exclusion of financial records emanating from Western Union Bank or telephone communications intercepted by the Dutch authorities.[103] In the *Ntaganda* case, the parties submitted from the bar table a series of audio and video excerpts for admission. The Trial Chamber assessed the probative value of each of the presented items and declined to admit certain video excerpts whose probative value was considered very low, while the parties had failed to prove the time and place where the excerpts were shot.[104] Besides these exceptions, the ICC has traditionally been criticized for deferring the decision on the admission of evidence to the final judgment.[105]

Ruling late on the admissibility of evidence may have a prejudicial effect for the party who needs to challenge the reliability and probative value of the evidence presented by its counterpart. For this reason, a group of independent experts tasked by the International Bar Association to put forward some recommendations to the ICC on how to improve equality of arms in proceedings, suggested amending Rule 64 of the Rules of Procedure and Evidence in order to avoid deferrals on the examination of the admission of evidence until deliberation, and established that:

> In the absence of prompt determinations on admissibility of evidence in these cases, the defence has had the onerous burden of responding to all evidence submitted, regardless of its relevance or probative value, and without a clear understanding of how it relates to the charges in the prosecution's case.[106]

Digital evidence adduced by the parties may be complex, highly voluminous, and time-consuming to examine and challenge. The risk of forgery of the sources of evidence, coupled with the risk of

[99]See Freeman, *supra* note 4, at 292–3.

[100]*The Prosecutor v. Al Hassan*, Second Decision on the Introduction of Prior Recorded Testimonies Pursuant to Rule 68(3) of the Rules, ICC-01/12-01/18-1267-Red, 26 January 2021, para. 24.

[101]See Freeman, *supra* note 4, at 292–3.

[102]A. Koenig and L. Freeman, 'Open Source Investigations for Legal Accountability: Challenges and Best Practices', in Dubberley, Koenig and Murray, *supra* note 64, at 334–5.

[103]Rome Statute, Art. 69(4). *The Prosecutor v. Jean-Pierre Bemba Gombo et al.*, Dec. on Requests to Exclude Western Union Documents and other Evidence Pursuant to Article 69(7), ICC-01/05-01/13, 29 April 2016.

[104]*The Prosecutor v. Bosco Ntaganda*, Dec. on Prosecution's Request for Admission of Documentary Evidence, ICC01/04-02/06-1838, 28 March 2017, para. 63.

[105]Amnesty International, 'Admitting Mistakes on Admitting Evidence – It's Not Too Late for the ICC to Get It Right', 4 May 2018, available at hrij.amnesty.nl/icc-bemba-et-al-judgment-admitting-mistakes-on-admitting-evidence/.

[106]International Bar Association, Recommendations of the International Bar Association ICC & ICL Programme to the Independent Expert Review of the International Criminal Court (April 2020), available at www.coalitionfortheicc.org/document/recommendations-international-bar-association-icc-icl-programme-independent-expert-review, at 16.

https://doi.org/10.1017/S0922156523000031 Published online by Cambridge University Press

bias due to many, and often unknown, users engaged in fact-finding activities, demand an *ex ante* and exhaustive examination of the admissibility of digital evidence. An inconsistent application of the rules on admissibility may result in the submission of an excessive pile of documentation whose relevance and relation to the charges have not been previously screened. Accordingly, objections that either party may raise on the provenance and reliability of digital materials should be addressed early in the proceedings. This would allow both the parties and the bench to narrow down the evidence that is relevant to the actual case for their preparation at trial.[107]

Therefore, clearer admissibility criteria, which provide for a higher threshold for the exclusion of evidence whose obtention contravenes internationally recognized human rights and national laws, as well as prompt rulings on their exclusion, would promote equality of arms in international criminal proceedings. This would allow both the prosecution and defence counsels to properly prepare for trial with a better use of their time and resources, which is essential to safeguard the equality of arms enshrined in Article 67(1) of the Rome Statute.

3.2.3.2 Assessment of digital evidence. Once the Chambers find the evidence admissible, Rule 63(2) of the ICC Rules of Procedure and Evidence gives the judges great flexibility to freely assess its weight and probative value.[108]

Digital evidence is often highly technical in nature and may require certain expertise to fully understand it.[109] For instance, call data records provide for a sequence of numbers that mean nothing to the conventional eye until they are properly analysed and interpreted through expert reports, which convert the records into call sequence tables. In the *Ayyash et al.* case before the STL, these call sequence tables were relevant evidence to track the co-defendants during their attack in Beirut on 14 February 2005 and to prove the assassination of former Lebanese Prime Minister Hariri and 21 others.[110]

When tendering digital evidence to the ICC Chambers, the parties may either request their admission from the bar table, or they would rather rely on experts or witnesses for the purposes of corroborating the authenticity and reliability of digital evidence.[111] While digital evidence, such as intercepted communications or video excerpts, may be *prima facie* admitted from the bar table, this does not afford them inherent reliability and probative value.[112] The ICC Chambers have established that, while there is not strict requirement for every piece of evidence be authenticated via expert report or witness statement, if the parties tender digital material into evidence from the bar table, they must accompany it with information that supports its authenticity and reliability,[113] e.g., information relating to the time and place a video was shot.

In the alternative, parties may present the evidence via expert reports or via witness statements. While the rules of *ad hoc* international criminal tribunals, namely the International Criminal Tribunal for the former Yugoslavia and the International Criminal Tribunal for Rwanda,[114]

[107] *The Prosecutor v. Alfred Rombhot Yekatom & Patrice-Edouard Ngaïssona*, Yekatom Defence Submission on the Conduct of the Trial, ICC-01/14-01/18, 15 May 2020, paras. 5–9.

[108] See Rules of Procedure and Evidence, *supra* note 44, Rule 63(2).

[109] E. Irving, R. Heinsch and S. Rewald, 'Using the Leiden Guidelines to Address Key Issues in Digitally Derived Evidence', *OpinioJuris*, 23 August 2022, available at www.opiniojuris.org/2022/08/23/using-the-leiden-guidelines-to-address-key-issues-in-digitally-derived-evidence/.

[110] *The Prosecutor v. Salim Jamil Ayyash*, Sentencing Judgment, STL-11-01/S/TC, 11 December 2020, paras. 11–27, 43, 140.

[111] L. E. Fletcher et al., 'An Overview of the Use of Digital Evidence in International Criminal Courts', (2013) *Salzburg Workshop on Cyber Investigations*, at 15.

[112] *The Prosecutor v. Turinabo et al.*, Decision on Prosecution Second Motion for Admission of Evidence from the Bar Table (Material Obtained from Registry and Seizures from Augustin Ngirabatware at the UNDF), MICT-18-116-T, 15 January 2021, at 3.

[113] *The Prosecutor v. Mr Jean-Pierre Bemba Gombo*, Decision on the Prosecution's Application for Admission of Materials into Evidence Pursuant to Article 64(9) of the Rome Statute, ICC-01/05-01/08, 8 October 2012, para. 159.

[114] Rule 94*bis* common to the International Criminal Tribunal for the Former Yugoslavia and the International Criminal Tribunal for Rwanda Rules of Procedure and Evidence.

https://doi.org/10.1017/S0922156523000031 Published online by Cambridge University Press

contained specific provisions regarding expert witnesses, the ICC Rules of Procedure and Evidence do not refer to the testimony of expert witnesses, nor do they establish the difference between expert and 'regular' witnesses.[115] Accordingly, the Chambers might elaborate their own requirements for allowing expert testimonies on a case-by-case basis.[116]

Forensic reports may be helpful to assist the Chambers understand the relevance of the raw data that have been submitted as evidence, to provide them with meaning, and to draw conclusions regarding their probative value. Additionally, the parties may call expert witnesses to appear in court to provide the bench with guidance on how to interpret the evidence presented.[117] When assessing the reliability of the expert's testimony, the Chamber may consider factors such as the expert's competence and impartiality, the forensic methodology followed, the consistency of the key findings, and the overall accuracy of the outcome.[118]

While expert reports may enlighten the Chambers for the purposes of interpreting digital evidence, judges are not always sufficiently skilled or trained at understanding the meaning behind the raw data selected and submitted as evidence. Forensic reports are not self-evident most of the times – in particular, when algorithms or AI-empowered technology is behind the selection of raw data, so judges may end up heavily relying on a party-appointed expert's testimony in order to weigh and assess evidence presented.[119] This has been sometimes criticized by judges themselves, by stating that conclusions and inferences must be drawn by the bench rather than by the expert's assistance.[120]

While drawing conclusions from the evidence presented is the Chambers' duty, experts may well assist the bench in interpreting certain facts and data that fall out of the judges' expertise. This interpretation, which may be biased to some extent by the expert's own methodology and assumptions, should certainly be subject to cross-examination and to the submission of a counter-report by the counterpart. It could also be counterbalanced by the Chambers' decision to request the appointment of an expert from the list of experts approved by the Registrar.[121]

Rather than relying on circumstantial testimonies, the Chambers have acknowledged that 'it is preferable for the Chamber to have as much forensic and other material evidence as possible. Such evidence should be duly authenticated and have clear and unbroken chains of custody'.[122] Therefore, greater emphasis should be placed on the analysis made by an expert in the relevant field, particularly when it comes to evidence that inherently requires a complex analysis, as digital evidence usually does.

4. Balancing a fair use of digital evidence at the ICC

The previous section has shown how the increasing use of digital evidence in the context of the ICC investigations and proceedings may make more burdensome the process of collecting, analysing, and assessing the evidence submitted by either party. The inherent voluminous and complex

[115]The Rome Statute and the ICC Rules of Procedure and Evidence refer to expert witnesses in certain regards, e.g., the appointment of experts to assist the OTP in the investigation of a concrete situation, or the protection of witnesses and experts. However, they do not provide for specific criteria on how to assess the testimony of expert witnesses.

[116]K. N. Calvo-Goller, *The Trial Proceedings of the International Criminal Court. ICTY and ICTR Precedents* (2006), Section 11.18, at 276.

[117]W. Jordash and L. Kulinowski, 'Vaguely Drawn Maps and Dimly Lit Paths: Rules Governing the Admissibility of Evidence at the *Ad Hoc* Tribunals (Part II)', in C. Rohan and G. Zyberi (eds.), *Defense Perspectives on International Criminal Justice* (2017), 445, at 451.

[118]*The Prosecutor v. Thomas Lubanga Dyilo*, Judgment pursuant to Article 74 of the Statute, ICC-01/04-01/06, 14 March 2012, para. 112.

[119]See Freeman, *supra* note 4, at 297.

[120]*The Prosecutor v. Kordic and Others*, ICTY Case No. 95–14/2, Official Transcript, 28 January 2000, at 13269.

[121]Regulation 44 of the Regulations of the Court, ICC-BD/01-05-16 (as amended on 12 November 2018).

[122]*The Prosecutor v. Laurent Gbagbo*, Decision Adjourning the Hearing on the Confirmation of Charges Pursuant to Article 61(7)(c)(i) of the Rome Statute, ICC-02/11/01/11, 3 June 2013, para. 27.

https://doi.org/10.1017/S0922156523000031 Published online by Cambridge University Press

nature of digital materials require the use of more resources to ensure the reliability and the sound interpretation of its content. Lack of sufficient resources and time constraints may widen the gap between the prosecution and the defence, thus undermining the equality of arms principle in international criminal proceedings.

As previously stated under Section 3.2, a disbalance in the opportunities afforded to either party by the introduction of digital evidence may arise at three different stages: when collecting the sources of digital evidence (Section 4.1); when analysing the materials collected (Section 4.2); and when the bench decides over the admissibility, the weigh and the probative value of the evidence presented (Section 4.3). For each of these stages, this section aims at offering some guidelines that may be introduced in the practice of the ICC to alleviate the burden that digital evidence may bring about, thus enhancing equal opportunities to both parties to the proceedings.

4.1 Enhancing equality of arms in the access and collection of digital sources of evidence: Disclosure obligations of digital materials

From the obstacles concerning the accessibility of sources of evidence which were highlighted in Section 3.2.1 above, it follows that defence teams will depend, to some extent, on the evidence gathered by the OTP when fulfilling its prosecutorial duty to investigate both incriminating and exonerating evidence under Article 54 of the Rome Statute, as well as on the disclosure of information that is material for the defence strategy. The defence may also want to deploy its own investigative capacity to collect new exonerating material. In that regard, while the defence may have access to privileged information from the accused that allows counsels to narrow down the search of materials that may serve as evidence, it may also encounter a more limited access to third-party resources, as compared to the OTP.

According to the Chambers Practice Manual, all exonerating evidence in possession or control of the Prosecutor must be disclosed 'as soon as practicable' and on a continuous basis.[123] However, the ICC's practice regarding disclosure has been inconsistent, and it is a cause for concern how little time is given to defence counsels to adequately prepare their case.[124]

When dealing with digital evidence, whose collection and analysis can be particularly burdensome and time-consuming, it becomes essential that disclosure obligations be carried out at the earliest stage possible after the suspect's first appearance (and, in particular cases, even before), and on a continuous basis.[125] Materials disclosed by the prosecution should encompass those that may potentially either cast doubt on the reliability of the prosecution's case – be it because of their provenance, their preservation, or their content, or help proving exonerating circumstances for the defence, safe for those that may impair the development of investigations in progress.

While the prosecution may enjoy certain discretion when deciding which evidence is material to the defence's case, the Pre-Trial Chamber should only take into consideration the evidence that has been disclosed for the purposes of making a decision on the confirmation of charges.[126] If the prosecution does not make an adequate and timely disclosure of materials that are relevant for the defence's case, the Trial Chamber may take this into consideration at a later stage, when deciding over the prejudice that the undisclosed evidence may cause to the defence, pursuant to Article 69(4) of the Statute.

[123]ICC, Chambers Practice Manual (May 2017), 10.

[124]See, for instance, the problems regarding disclosure in *The Prosecutor v. Thomas Lubanga Dyilo*, Decision on the Prosecution's Urgent Request for Variation of the Time-Limit to Disclose the Identity of Intermediary 143 or Alternatively to Stay Proceedings Pending Further Consultations with the VWU, ICC-01/04-01/06, 8 July 2010, as well as in *The Prosecutor v. Francis Kirimi Muthaura and Uhuru Muigai Kenyatta*, Prosecution Notification of Withdrawal of the Charges Against Francis Kirimi Muthaura, ICC-01/09-02/11, 11 March 2013, para. 10.

[125]See ICC, *supra* note 123, at 9–10.

[126]Ibid., at 11.

https://doi.org/10.1017/S0922156523000031 Published online by Cambridge University Press

In any event, in the communication of the disclosed evidence to the Pre-Trial Chamber, both parties should be present when submitting the disclosed 'raw data'. On a relevant note, when it comes to digital datasets or excerpts, both parties should be aware of the selection process that the counterpart will make out of the whole dataset, as well as of the criteria and the methodology used in order to extract and analyse the data. For instance, if a series of call data records are disclosed by the prosecution, the defence should be aware of how these records will be selected and sequenced, even if it is not obliged to disclose any other internal documents, reports, or analyses of the call sequence tables.[127]

On the other hand, providing that the defence wants to carry out its own research for exonerating material, defence teams must be afforded sufficient judicial guarantees to be granted access to external sources of evidence. Considering that the defence does not benefit from a wide network to collect external evidentiary sources, e.g., coming from digital service providers, the ICC Pre-Trial Chamber should be empowered to order third parties to exhibit data that are considered material to the defence's case, providing that these requests comply with data privacy international and national laws.[128] The ICC Chambers have not yet been vested with enforcement powers to compel the exhibition and submission of evidence in hands of a third-party through binding orders.[129] Should that be the case, the request by the defence would undergo a previous judicial deliberation on the need to access those records, along with their potential relevance to the case and any prejudice which might be caused to third parties therefrom. That way, the opportunities afforded to both parties in terms of accessibility to external sources of evidence would be levelled off.

4.2 Enhancing equality of arms in the analysis of digital evidence

In relation to the difficulties arising from the verification and analysis process that digital materials often require, the reflections laid out in Section 3.2.2 above pointed to the apparent lack of resources and institutional support as the main contributing factors for the impairment of fair trial rights. While it is certain that the tight budget that the ICC is subject to has a clear impact on the overall investigation of international crimes, and affects all different branches of the institution alike, the financial independence and the limited administrative assistance may leave defence counsels one step behind in the procurement of experts. Digital evidence requires sophisticated expertise in order to be decrypted, selected, and analysed, and thus it is likely that more resources will need to be spent for those purposes.

When assessing the way in which the ICC may offer an improved institutional backup to defence teams, the proposed approach is twofold. On the one hand, the budgetary resources afforded to investigation teams should envisage that certain investigation tools – which may include, e.g., big data analytics technologies, data management tools, or eDiscovery tools, may be equally used and shared by both the OTP and defence teams, so that the defence may have access to the same search engines as the prosecution does for the purposes of processing and selecting the sources of digital evidence.

On the other hand, the Pre-Trial and Trial Chambers could play a more inquisitorial role should they notice that more institutional resources are needed to process certain types of evidence. For instance, whenever difficulties or inconsistencies arise in the scrutiny of the digital evidence provided by the parties, the Chambers could use their competence under Regulation 44 of the Regulations of the Court to appoint and instruct on its own motion an independent, judicial expert witness, which might shed light on the analysis and interpretation of evidence.[130]

[127]See Leiden Guidelines, *supra* note 9, Section E.2, at 42–3.

[128]Arts. 56 to 58 of the Rome Statute allow the Pre-Trial Chamber to issue judicial orders and arrest warrants during the course of the investigation, if it is formally requested by the OTP.

[129]J. K. Cogan, 'International Criminal Courts and Fair Trials: Difficulties and Prospects', (2002) 27 *Yale Journal of International Law* 111, at 123–4.

[130]Regulation 44(4) of the Regulations of the Court, ICC-BD/01-05-16 (as amended on 12 November 2018).

https://doi.org/10.1017/S0922156523000031 Published online by Cambridge University Press

4.3 Enhancing equality of arms in the admissibility and the assessment of digital evidence

The review on the rules of admissibility and assessment of evidence in ICC proceedings that was set out in Section 3.2.3 above pointed out two main concerns regarding the Chambers' practice in this context: (i) the possibility of deferral on the decision of admissibility or exclusion of evidence; and (ii) the lack of reliance on expert reports in court. Although these practices may have an impact on the introduction of any type of evidence in court, they become particularly relevant when the Chambers need to assess the weigh and probative value of digital evidence, for the interpretation and understanding of this kind of evidence requires a greater investment on resources, time, and expertise.

The rules governing the ICC criminal proceedings offer great flexibility as far as the submission, admissibility, and assessment of evidence are concerned. However, when dealing with evidence that is inherently complex and highly voluminous in nature, a lack of rigorous criteria for the admissibility and assessment of evidence may be notably prejudicial to the rights of the accused. A deferral of the decision on the admission or exclusion of evidence leaves the parties (and, in particular, the defence) with the task of challenging all the evidence submitted by the counterpart at trial, without prior knowledge of its relevance to the charges and counts. Challenging such a high volume of digital materials seems impracticable within such a tight timeframe and resources, while proving inefficient in the interests of procedural economy.

It is imperative to advocate for a prompt decision on admissibility of evidence, particularly when the confrontation of the evidence submitted is highly onerous for the opposing counsel. An obligation of the Chambers to rule early on admissibility may be drawn from Rule 64 of the Rules of Procedure and Evidence.[131] Judge Eboe-Osuji is of the opinion that, if parties have an obligation to raise objections to the evidence as soon as it is submitted by the counterpart pursuant to Rule 64, that implicitly compels judges to rule upon those evidentiary objections.[132] When deciding over their admissibility, judges must strictly apply the criteria established in Article 69(4), relating to the probative value, relevance, and potential prejudice that the submitted evidence may cause to the rights of the accused.[133] Knowing upfront which pieces of evidence are admissible would contribute to the overall efficiency of the proceedings, thus allowing the defence to optimise their available resources while focusing on only examining those items which are relevant to the outcome of the case.

Lastly, when assessing digital evidence that is particularly hard to interpret and understand, the evidence should be tendered via expert reports and witnesses. In fields that fall out of the judges' expertise, expert witnesses may enlighten the bench by explaining the methodology used for interpreting the dataset. Reliance on expert reports would not substitute the bench's judgement whatsoever. On the contrary, forensics should be able to make the analysis of the evidence more accessible to the judges, thus providing sufficient elements to the judges to comprehend the weight and probative value that should be afforded to digital materials. In any event, the interpretations provided by experts may be supported by cross-examination of the expert witnesses, and, if necessary, be counterbalanced by additional expert reports that contrast the methodology and key findings put forward by the original report.

[131]Rule 64(1) of the Rules of Procedure and Evidence states that: 'An issue relating to relevance or admissibility must be raised at the time when the evidence is submitted to a Chamber ...'.

[132]*The Prosecutor v. Jean-Pierre Bemba Gombo*, Judgment pursuant to Article 74 of the Statute (Separate Opinion of Judge Eboe-Osuji), ICC-01/05-01/08-3636-Anx3, 14 June 2018, para. 302.

[133]*The Prosecutor v. Jean-Pierre Bemba Gombo*, Judgment pursuant to Article 74 of the Statute (Separate Opinion of Judge Van den Wyngaert and Judge Morrison), ICC-01/05-01/08-3636-Anx2, 8 June 2018, para. 18.

https://doi.org/10.1017/S0922156523000031 Published online by Cambridge University Press

5. Concluding remarks

The article has argued how the increasing reliance on digital sources of information and digital evidence in court may put additional burdens on the parties to verify their authenticity and reliability for their subsequent use in court. The inherently complex nature of digital evidence, which may often require the use of analytics to examine and manage large volumes of datasets, makes the use of digital evidence a particularly resource-intensive task. Accordingly, there is a risk that the asymmetry between the prosecution and the accused throughout the criminal proceedings before the ICC is widened. This might put in jeopardy the conduction of a fair trial, thus undermining the principle of equality of arms.

The main proposals which have been put forward are directed at balancing the procedural opportunities afforded to both parties, by enacting positive discrimination measures which favour the weaker party whenever it may encounter major difficulties to manage the use of digital sources of evidence. A more robust institutional backup, along with a proactive and inquisitorial role of the judges, can alleviate the excessive burdens that the management of digital evidence may put on defence teams. More precisely, the approach that has been taken focuses on the three main stages that the parties will go through in proceedings before the ICC: (i) the collection and preservation of evidence; (ii) the examination of the evidence; and (iii) the admissibility of the evidence and the establishment of its probative value.

As has been previously developed, some of the practices that may be implemented in order to seek equal procedural opportunities for both parties would be the following:

1. First, disclosure obligations should be strictly complied with by both parties, and the disclosure process should be led by the Chambers, in order to ensure that both parties have access to the disclosed raw data and be present in the selection process of such data. Also, the Chambers should be empowered to order third parties to grant defence teams access to digital sources of evidence whenever they are deemed essential for their defence strategy.
2. Second, adequate expertise and sufficient resources should be afforded to defence teams in order to conduct a proper analysis and verification process of the digital sources of evidence collected, by granting them access to efficient analytic software and management tools.
3. Third, an early ruling on the admissibility of evidence, together with a rigorous application of the criteria set out in the Rome Statute and the ICC Rules of Procedure and Evidence on the admissibility of evidence, would be essential in the interests of efficiency and procedural economy. This would allow the parties to direct their efforts to verify and challenge the evidence which is relevant to the case, which will in turn save time and resources that need to be invested to confront complex and voluminous digital evidence. Additionally, the Chambers may benefit from the reliance on expert reports that provide for an interpretation of the digital evidence presented, which might be cross-examined in trial and through counter-reports.

All in all, providing sufficient guarantees to ensure fair trial rights in proceedings that increasingly rely on digital evidence in court is in the interests of all. Digital pieces of evidence will have an increasing relevance in future prosecutions in international criminal tribunals. Practices that enhance equality of arms in international criminal proceedings will ensure that both parties may equally benefit from the use of information of digital origin and technological tools. This may, in turn, contribute minimizing the backlash coming from the states of nationality of the accused persons, thus enhancing institutional co-operation with the ICC. Overall, the implementation of these safeguards when the parties are confronted with digital evidence may ultimately strengthen the efficiency and legitimacy of the ICC proceedings.

Cite this article: de Arcos Tejerizo M (2023). Digital evidence and fair trial rights at the International Criminal Court. *Leiden Journal of International Law* **36**, 749–769. https://doi.org/10.1017/S0922156523000031