UDK 341.4:004.7]:342.7
Original scientific paper

# DIGITAL EVIDENCE IN INTERNATIONAL CRIMINAL PROCEEDINGS AND HUMAN RIGHTS CHALLENGES*

**Chiara Ragni, PhD, Full Professor**
University of Milan, Department of International,
Legal, Historical and Political Studies
Via Conservatorio 7, 20 122 Milan, Italy
chiara.ragni@unimi.it

***ABSTRACT***

*Digital technologies offer great opportunities in every field of life, including in criminal proceedings, where gathering evidence using digital or computer devices is an important contribution to the investigation of crimes, especially at the international level. Digital evidence is particularly important in the prosecution of international crimes due both to their complexity and to its ability to overcome hurdles that international judges must overcome when fact-finding relates to conduct that occurred far from the seat of the court. While the of digital evidence is increasing, however, questions have arisen concerning both its admissibility and of its reliability, as the jurisprudence of the International Criminal Court (ICC) and other international criminal tribunals makes clear. The use of digital evidence may also raise concerns for the respect of due process standards and the right to private life. In the absence of specific international legal rules that deal with the matter, the purpose of this contribution is to identify the most pressing issues through an examination of the case law of international tribunals and to infer potential solutions and best practices to consider in developing international human rights based procedural standards.*

***Keywords:*** *digital evidence; international criminal proceedings; international crimes; law of evidence; admissibility; reliability; human rights standards; right to private life; right to a fair trial*

* This paper is co-funded by the Erasmus+ Programme of the European Union. The paper reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

## 1. INTRODUCTION

In recent decades, criminal investigators and judges have increasingly relied on digital technologies as a means of supporting fact-finding in relation to the commission of crimes, both in international and in domestic proceedings. In the international context, the availability of a broad range of digital tools, like video recordings, intercepted communications, open-source on-line information, aerial drone footage, social media content and geo-referenced field documentation has opened up broad opportunities to strengthen investigations of grave human rights abuses.[1]

The use of digital technologies in the prosecution of international crimes has allowed international criminal tribunals to overcome some of the hurdles they must face due to their distance (both geographical and temporal) from crime scenes and their dependence upon the cooperation of domestic authorities. In most cases, the difficulty of collecting some evidence, like witnesses' testimonies, for example, is even exacerbated by security reasons, especially in the contexts of political disorder or of armed conflict – contexts in which most international crimes are committed. Modern technologies and devices may help fill evidentiary gaps,[2] despite the fact that Tribunals must continue to rely on the cooperation not only of states but also of private entities, the activities of which provide them with large amounts of data.

The use of video and photographs as evidence in international legal proceedings is not new. It dates back to the Nuremberg trial, when live footage of the final days of World War II was shown in the courtroom and had a significant impact on the judges' assessment of the facts. As new technologies have developed, both in the field of forensic medicine and in the collection and storage of data and metadata, their importance in international criminal proceedings has grown, as we see from the case law of both the *ad hoc* International Criminal Tribunals[3] and, subsequently, of the International Criminal Court (ICC), both of which rely on ever more sophisticated tools.[4]

---

1 Land, M.; Aronson, J. (eds.), *New Technologies for Human Rights Law and Practice*, Cambridge University Press, Cambridge, 2018, spec. p. 125 ff.

2 Harmon, M.B., *Prosecuting Massive Crimes with Primitive Tools: Three Difficulties Encountered by Prosecutors in International Criminal Proceedings*, Journal of International Criminal Justice, Vol. 2, No. 2, 2004, pp. 403–426.

3 As to the ICTY, see for example *Prosecutor v Tolimir*, Case No. IT-05-88/2-T, Judgment, 12 December 2012, as regards the use of DNA analysis for the identification of the "Srebrenica-related missing" (*ibid.*, para 49 ff.) and of intercepted communications and aerial imagery (para 63 ff.) as evidence. For the ICTR, cf. *Prosecutor v Bagosora*, Case No. ICTR-98-41-T, Trial Judgment and Appeals Judgment, 8 December 2008 and 14 December 2011, respectively paras 2029-2031, 460, where the judges based on video footage their findings on the role of the defendant as the Rwandan Minister of Defence.

4 Freeman, L., *Digital Evidence and War Crimes Prosecutions: The Impact of Digital Technologies on International Criminal Investigations and Trials*, Fordham International Law Journal, Vol. 41, No. 2, 2018, pp. 283-336.

Although the potential of digital evidence and methods to assist in the prosecution of international crimes is undeniable, they also raise significant issues of both admissibility and reliability. As to the former, problems of admissibility may arise, for example, in the event data were collected in violation of privacy rights, which are protected by human rights legislation. As to the latter, one need only consider data posted on social media to perceive the concrete risks that they will be quickly removed before they can be preserved by investigators, or that they may represent fake or inaccurate information.

In light of these premises, then, the aim of the paper is to: i) examine the case law of International criminal tribunals, with a focus on the ICC, in order to identify cases in which the judges based their findings – at least in part – on digital evidence;[5] ii) identify the most problematic issues concerning the admissibility and reliability of this kind of evidence in light of the Rules of Procedure and Evidence (RPE) of International criminal tribunals and especially of the ICC; iii) investigate, with regard to the question of admissibility, how the international criminal tribunals have balanced the probative value of digital evidence with the respect of human rights.

## 2. THE INCREASING USE OF DIGITAL EVIDENCE IN INTERNATIONAL CRIMINAL PROCEEDINGS AND ITS ADVANTAGES

The jurisprudence of the international criminal tribunals reveals that, especially in recent years, they are increasingly using digital technologies for fact-finding purposes. As anticipated in the premise, in fact, digital evidence in international criminal proceedings has allowed the tribunals to address some of the problems that the prosecution of international crimes generally entails. In addition to the obstacles to collecting evidence mentioned above, digital tools are also well-tailored for addressing the specific features of international crimes. The complexity of such crimes due to the fact that they are not limited to a single act, but occur

[5] Even if there is no legal definition of digital evidence, it may be assumed that the term includes "any data [of value to an investigation] resulting from the output of an analogue device and/or a digital device of potential [probative] value that are generated, processed, stored or transmitted using any electronic device". European Commission, *European Data Informatics Exchange Framework for Courts and Evidence*, European Evidence Project, available online at [www.cordis.europa.eu/project/id/608185/reporting/de], Accessed 12 January 2022. Digital, or electronic, evidence has also been described by scholars dealing with the matter as "any probative material stored or transmitted in digital form, … which can be used in legal proceedings before a court in order to prove a fact according to the required standard of proof". For this definition, see Roscini, M., *Digital Evidence as a Means of Proof before the International Court of Justice*, Journal of Conflict & Security Law, Vol. 21, No. 3, 2016, pp. 541-554.

as a part of a greater course of conduct and require proof of contextual as well as specific elements.[6]

In such cases, aerial and satellite images and video footage may be fundamental for demonstrating the existence of mass and grave destruction or killings, the movement of people or troops, and devastated areas. For example, the International Criminal Tribunal for the Former Yugoslavia (ICTY) made recourse, in the *Tolimir* case, to satellite imagery provided to the Prosecutor by the US military to prove the presence of gravesites and reburial activities, buildings and vehicles, large groups of prisoners, and bodies at particular locations. In *Krstić* aerial images were used for proving the mass and grave killings committed in Srebrenica.[7]

Examples of the use of satellite images as evidence of facts may be also found in the practice of the ICC. In the *Darfur* cases, for example, the Prosecutor made extensive reference to the report of the Commission of Inquiry, designated to ascertain the facts as they occurred during the Government's violent campaign against the rebels. The report, in turn, mostly relied on satellite images provided by human-rights organisations, which used them to detect the destruction and burning of villages, and the movement of refugees.[8] In the *Al Mahdi* case, the Prosecutor presented a significant amount of open source evidence, including satellite images found on Google Earth.[9] Although, as discussed below, the use of this kind of image as evidence may pose issues of reliability, their introduction into the proceeding reveals the pervasiveness internet and digital tools have reached even in the

---

6 On the advantages of digital evidence in prosecuting international crimes see Freeman, L., *Prosecuting Atrocity Crimes with Open Source Evidence: Lessons from the International Criminal Court*, in: Dubberley, S.; Koenig, A.; Murray, D. (eds.), Digital Witness - Using Open Source Information for Human Rights Investigation, Documentation, and Accountability, Oxford University Press, Oxford, 2019, pp. 48-67.

7 "Aerial photographs, taken on 17 July 1995, of an area around the Branjevo Military Farm, show a large number of bodies lying in the field near the farm, as well as traces of the excavator that collected the bodies from the field". The executions in Kozluk must have occurred between 14 July and 17 July 1995, given that aerial images show the mass grave in the Kozluk area was created prior to 17 July 1995 and the prisoners were not transported to the zone of responsibility of the Zvornik Brigade until 14 July 1995". *Prosecutor v Radislav Krstic*, Case No. IT-98-33, Judgement, 2 August 2001, respectively paras. 237 and 253.

8 International Commission of Inquiry on Darfur, *Report of the International Commission of Inquiry on Darfur to the United Nations Secretary-General*, 2005, paras. 183 and 301, [https://www.legal-tools.org/doc/1480de/pdf/], Accessed 12 January 2023. On the use of satellite imagery as evidence in the jurisprudence of the ICC see Sandalinas, J., *Satellite Imagery and its use as Evidence in the Proceedings of the International Criminal Court*, Zeitschrift Für Luft-Und Weltraumrecht: Vierteljahresschrift Des Instituts Für Luft- Und Weltraumrecht Der Universität Köln, Vol. 64, No. 4, 2015, pp. 666-675.

9 *Prosecutor v Al Mahdi*, Case No. ICC-01/12-01/15-171, Decision on the confirmation of charges against Ahmad Al Faqi Al Mahdi, 24 March 2015. For a comment see Freeman, L., *Prosecuting…*, *op. cit.*, note 6, p. 316 ss.

forensic context. This pattern continues in the use of modern technologies, and, in particular, of aerial and satellite images of bodies on the streets of Ukrainian cities, to document the killing of civilians by the Russian army and, therefore, to indicate the commission of war crimes.

Digital evidence has also proven relevant for demonstrating a person's involvement in a criminal conspiracy or in planning, ordering and directing the perpetration of international crimes, the commission of which is generally the result of a precise policy or of criminal design. Intercepted communications are important for this purpose, and have been used extensively by all the International criminal tribunals.

In *Blagojević* and *Jokić*, intercepted communications were presented by the Prosecutor of the ICTY as evidence of the "communications between officers and soldiers of the VRS Main Staff, Drina Corps and subordinate brigades during the weeks before, during and after the fall of Srebrenica… Indeed, taken individually, certain intercepts provide direct evidence of the accused's knowledge of and/or participation in the forced removal of civilian Muslims from Srebrenica and the subsequent massacre of Srebrenica's Muslim men. Perhaps more importantly, as a whole, the intercept evidence tells the story of the VRS military participation in the attack on Srebrenica and the events that follow, and forms an important part of the mosaic of evidence to be introduced by the Prosecution".[10] In *Popović*, intercepted communications were used to demonstrate the chain of command and provided a narrative of the VRS attack on Srebrenica and the events that followed.[11]

Telecommunications evidence, including call data records and cell site information, were presented before the Special Tribunal of Lebanon (STL), the sole international court to have jurisdiction over the crime of terrorism, to prove the preparatory acts leading up to the terrorist attack which killed the Prime Minister of Lebanon, Rafiq Hariri on 14 February 2005. In *Ayyash et a.*, call data records served to prove both communications among the accused persons and that the network mobiles were engaged in Mr Hariri's surveillance and assassination.[12]

---

10 *Prosecutor v Blagojević and Jokić*, Case No. IT-02-60-T, Decision on the admission into evidence of intercept-related materials, 18 December 2003, para. 4.

11 *Prosecutor v Popović et al*, Case No. IT-05-88-T, Decision on Admissibility of Intercepted Communications, 7 December 2007.

12 *Prosecutor v Ayyash et al*, Case No. STL-11-01, Decision on Motions for the Admission of the Call sequence tables related to the five colour-coded mobile telephone groups and networks call sequence tables, 31 October 2016. See Fremuth, M., *Prosecutor v Ayyash et al (Special Trib. Leb.)*, International Legal Materials, Vol. 60, No. 3, 2021, pp. 357-447.

The ICC has also relied on intercepted communications. In *Ongwen*, the Prosecutor presented Lord's Resistance Army (LRA) radio communications intercepted by Ugandan security agencies to the Chamber as evidence. In particular, it submitted to the Court a logbook summary of the information intercepted, which had been prepared by interceptors at the end of a series of interceptions, and which aimed to transcribe and summarize in English the content of the communications (which were predominantly in Acholi or Luo, two local dialects). The interceptors gave their logbook entries to their commanders, who transmitted the intercepted communications to Kampala to inform the Uganda People's Defence Force's broader military operations. All the completed recordings and logbooks were securely stored, either at the sites of interception or in Kampala.[13] What the Prosecutor submitted to the Chamber was the product of both a selection made by the Uganda governmental authorities when they transmitted the records and notes taken by interceptors and of a process of "enhancement" of audio recordings.[14] To overcome doubts and criticisms that accompanied the submission of intercepted communications, a fundamental role was played by the so-called 'intercept witnesses'—witnesses able to discuss the interception's operations as well as specific intercepted communications. The witnesses were called by the Prosecutor to testify before the Court with the aim, first, of identifying the speakers and confirming the correspondence of the audios with the transcripts, on, second, of explaining the methodology used to enhance the audio for the purpose of criminal proceedings. Leaving for aside all these issues, which will be better discussed here below, it is worth noting that intercepted communications were used as evidence of Ongwen's rank as a brigade commander and of his "interactions, in particular of the LRA's radio communication network, during which intentions to harm civilians on account of their perceived association with the Government of Uganda were discussed. In addition, the Chamber finds support for this conclusion in its findings in relation to Dominic Ongwen's involvement in the four attacks relevant to the charges."[15]

Notwithstanding the increasing importance of digital evidence in international criminal proceeding, defendants have often challenged its admissibility and reli-

---

13 *Prosecutor v Dominic Ongwen*, Case No. ICC-02/04-01/15, Judgment, 4 February 2021, para. 614 ff.

14 As we will see in greater detail (*infra*, sections 3-4), the procedure followed for this kind of evidence raised several concerns as regards its reliability, that were brought by the Defence to the attention of the Court. See in this regard the analysis made by Marchesi, D., *Intercepted Communications in the Ongwen Case: Lessons to Learn on Documentary Evidence at the ICC*, International Criminal Law Review, Vol. 22, No. 5-6, 2022, pp. 920-940.

15 *Ongwen*, *op. cit.*, note 13, paras. 1146-1147. For more examples see Freeman, L.; Vazquez Llorente, R., *Finding the Signal in the Noise: International Criminal Evidence and Procedure in the Digital Age*, Journal of International Criminal Justice, Vol. 19, No. 1, 2021, pp. 163–188.

ability on various grounds pertaining to the authenticity of the piece, to the source of the information or the chain of transmission, and to the procedure used to collect the evidence.

In *Tolimir*, for example, the accused challenged the reliability of satellite images, on the grounds that no evidence was presented concerning their origin, the method of their creation, the manner of their editing, how to interpret them or whether they were delivered to the Prosecution in their original form or in a modified version.[16] In *Ongwen*, the Defence contended that the majority of the intercepted material was irrelevant and that there were significant discontinuities in the tapes.[17] In the same case, it challenged the use of video footage as evidence, arguing that it was collected in violation of human rights and, therefore, as we will better explain here below, in contravention of the ICC Statute.[18] Human rights arguments were also raised in *Ayyash et a.* concerning the admissibility into evidence of call sequence tables, which were gathered, according to the Defence, in violation of the right to privacy.

## 3. QUESTIONS OF ADMISSIBILITY AND RELIABILITY OF DIGITAL EVIDENCE BEFORE INTERNATIONAL CRIMINAL TRIBUNALS

The Statutes of the international criminal tribunals do not contain any specific provision on digital evidence, which is also not defined by their rules of evidence. Concerning its admissibility, the Rules of Procedure and Evidence (RPE) of international tribunals do not include specific provisions on this particular type of evidence, the admissibility and reliability of which are therefore governed by general norms. These grant judges a broad margin of discretion in the matter.

Rule 89 (C) of the ICTY and of the International Criminal Tribunal for Rwanda (ICTR) give the Chamber the power to admit any relevant evidence which it deems to have probative value.[19] Article 89(D) of the ICTY RPE further provides that a Chamber may exclude evidence if its probative value is substantially out-

---

16 *Tolimir*, *op. cit.*, note 3, paras. 67-68. The Prosecutor was actually not allowed to share any information relating to the "technical or analytical sources, methods, or capabilities of the systems, organizations, or personnel used to collect, analyse, or produce these imagery-derived products".

17 *Prosecutor v Ongwen*, Case No. ICC-02/04-01/15, Public Redacted Version of 'Corrected Version of "Defence Closing Brief", 13 March 2020, paras. 232-233.

18 *Ongwen*, *op. cit.*, note 13, para. 54 ff.

19 International Criminal Tribunal for the former Yugoslavia, Rules of Procedure and Evidence (last amended in 2015, adopted on 11 February 1994), IT/32Rev.50 (hereinafter 'ICTY RPE'); International Criminal Tribunal for Rwanda, Rules of Procedure and Evidence (last amended in 2015, adopted on 29 June 1995), Rule 89(D).

weighed by the need to ensure a fair trial. The same principle has been applied by the ICTR, even if it is not expressly stated in its rules.[20]

Like the general ICTY and ICTR rules, Article 69(4) of the Rome Statute of the ICC provides that "the Court may rule on the relevance or admissibility of any evidence, taking into account, *inter alia*, the probative value of the evidence and any prejudice that such evidence may cause to a fair trial or to a fair evaluation of the testimony of a witness […]". Article 69 (7) of Rome Statute specifies that "[e] vidence obtained by means of a violation of this Statute or internationally recognized human rights shall not be admissible if: (a) The violation casts substantial doubt on the reliability of the evidence; or (b) The admission of the evidence would be antithetical to and would seriously damage the integrity of the proceedings". The same provisions are included in the STL Statute and in the RPE.[21] Although some slight differences exist among the evidentiary rules that each tribunal applies, some common principles may be inferred from the above provisions.

First, it is for the judges to rule on the admissibility and relevance of all evidence. In so doing, they may freely assess all types of evidence submitted, enjoying a significant degree of discretion. However, – and this is the second principle that may be drawn from the rules above - any item to be admitted as evidence must satisfy some requirements: i) relevance to the case, which shall be assessed, according to Articles 69(9)(a) and 69(4) of the ICC Statute, considering how much the "evidence tendered makes the existence of a fact at issue more or less probable"; ii) probative value, which points to its utility in proving an important part of the case and to its relevance in determining a fact or issue;[22] iii) both these conditions shall be balanced against any prejudicial effect that could be caused to the proceeding by the admission of the evidence. As to this last point, judges must be satisfied that, *inter alia*, evidence has not been obtained through means that amount to a violation of internationally recognized human rights, as this may jeopardize both its reliability and the integrity of the proceedings.

---

20 See on that the *Report on Digitally Derived Evidence In International Criminal Law*, Part of the digitally derived evidence Project, Leiden University, 2019, p. 22 ff., [https://leiden-guidelines.com/assets/DDE%20in%20ICL.pdf], Accessed 12 January 2023.

21 Art. 21 para. 2 states: "A Chamber may admit any relevant evidence that it deems to have probative value and exclude such evidence if its probative value is substantially outweighed by the need to ensure a fair trial". This provision is furtherly specified by Rule 162 RPE, that reads as it follows: "(A) No evidence shall be admissible if obtained by methods which cast substantial doubt on its reliability or if its admission is antithetical to, and would seriously damage, the integrity of the proceedings. (B) In particular, evidence shall be excluded if it has been obtained in violation of international standards on human rights, including the prohibition of torture".

22 Quelling, C., *The Future of Digital Evidence Authentication at the International Criminal Court*, Journal of Public & International Affairs, May 2022.

As mentioned above, digital evidence has been challenged in this last regard before the STL in *Ayyash et a.* and before the ICC in *Ongwen*.[23] In the former case, the Defence contended that the transfer of call data records from Lebanon to the United Nations International Independent Investigation Commission (UNIIIC), a commission established to investigate the murder of Rafiq Hariri, and to the Prosecution, was unlawful and arbitrary and that there had been violations of international human rights standards with regard to the right to private life. In *Ongwen*, the use of digital evidence was challenged on the grounds that it violated the right to a fair trial. It is worth noting that, in that case, the interceptions submitted by the Prosecutor were not made for purposes relating to a criminal investigation, but rather for security and military reasons. The materials transferred to the Prosecutor were, therefore, selected on the basis of the specific aim pursued by the Government, which was far from that of ensuring an objective investigation into the commission of international crimes; their admissibility as evidence raised human rights concerns in this regard with reference to due process standards.

### 3.1. Human rights standards and digital evidence

The law of evidence of international criminal tribunals generally refers to human rights standards without specifying further. This raises some questions about both which rights fall into the notion and their legal source.

The right to privacy is, as the cited cases clearly show, one of paramount concern when it comes to digital evidence, due to the fact that information is often collected using means that are likely to interfere in the private life of the person concerned. International criminal tribunals, starting with ICTY, have clearly stated that this right falls into the notion of "human rights standard" for the purposes of deciding on admissibility.[24] Concerning the legal source of the right, reference is generally made to Article 17 of the International Covenant on Civil and Political Rights, to Article 8 of the European Convention on Human Rights, and to Article 11 of the Inter-American Convention on Human Rights. According to the jurisprudence of both criminal and human rights tribunals, intercepts of private conversion and access to call data records may breach the right to privacy unless

[23] *Ongwen*, *op. cit.*, note 13, para. 57 ff.

[24] See for example *Ayyash* et al., *op. cit.*, note 12, para. 81; *Prosecutor v Radoslav Brdanin*, Case No. IT-99-36-T, Decision on the defence "objection to intercept evidence", 3 October 2003, spec. para. 31.; *Prosecutor v Thomas Lubanga Dyilo*, Case No. ICC-01/04-01/06, Decision on the confirmation of charges, 29 January 2007, para. 73, which reads as it follows: "…the right to privacy and to protection against unlawful interference and infringement of privacy is a fundamental internationally recognised right. However, it cannot be viewed as an absolute right in so far as these same instruments provide indications of what may be considered as a "lawful" interference with the fundamental right to privacy".

they respect certain guarantees.[25] The interception must be provided by the law, necessary under the circumstances, and proportional to the pursuit of a legitimate aim.[26] The European Court of Human Rights (ECtHR) has furtherly explained that the assessment shall be particularly rigorous where digital technologies are at issue. In *Amann v Switzerland*, it argued that "tapping and other forms of interception of telephone conversations constitute a serious interference with private life and correspondence and must accordingly be based on a 'law' that is particularly precise. It is essential to have clear, detailed rules on the subject, especially as the technology available for use is continually becoming more sophisticated".[27] In *Centrum för Rättvisa v Sweden*, the ECtHR added, with regard to bulk interception, that "while Article 8 of the Convention does not prohibit the use of bulk interception to protect national security and other essential national interests against serious external threats, and States enjoy a wide margin of appreciation in deciding what type of interception regime is necessary, for these purposes, in operating such a system the margin of appreciation afforded to them must be narrower and a number of safeguards will have to be present".[28]

Decisions on the admissibility of digital evidence that may raise human rights concerns should, therefore, be based on an overall assessment of whether the legal and procedural safeguards against abuse are sufficient and adequate.[29] In *Ayyash et*

---

25 *Malone v United Kingdom*, Application No. 8691/79, Judgment, 2 August 1984, para. 62; *Brđanin*, *op. cit.*, note 24, para. 30.

26 UN Human Rights Committee, General Comment 31, Nature of the General Legal Obligation on State Party to the Covenant, CCPR/C/21/Rev.1/Add. 13, 24 May 2004, para. 6; ECtHR, *Amann v Switzerland* Application No. 27798/95, Judgment, 16 February 2000, para. 69, which expressely regards the consistency of interception of phone conversations with Article ECHR 8.

27 *Amann v Switzerland*, para. 56.

28 The Court has developed the following minimum requirements that should be set out in law in order to avoid abuses of power: "(1) the nature of offences which may give rise to an interception order; (2) a definition of the categories of people liable to have their communications intercepted; (3) a limit on the duration of interception; (4) the procedure to be followed for examining, using and storing the data obtained; (5) the precautions to be taken when communicating the data to other parties; and (6) the circumstances in which intercepted data may or must be erased or destroyed". *Centrum För Rättvisa v Sweden*, Application No. 35252/08, Judgment, 25 May 2021, para. 178 ff.; in the same vein cf. [GC], *Big Brother Watch and Others v The United Kingdom*, Applications Nos. 58170/13, 62322/14, 24960/15, Judgment, 25 May 2021.

29 It is worth noting that recommendations on the necessity for States to adopt measures to ensure that the use of digital technologies does not affect human rights, and namely the right to private life was also issued by the UN General Assembly. On 18 December 2013 it adopted Resolution no. 68/167 on the right to privacy in the digital age (A/RES/68/167), in which, inter alia, it called upon States: "(a) To respect and protect the right to privacy, including in the context of digital communication; (b) To take measures to put an end to violations of those rights and to create the conditions to prevent such violations, including by ensuring that relevant national legislation complies with their obligations under international human rights law; (c) To review their procedures, practices and legislation regarding the

*al* the STL admitted into evidence call records that were submitted by the Prosecutor on the grounds that they met the conditions required by international law to comply with human rights standards.[30]

The question then arises as to whether, in the opposite case, where the court concludes that digital evidence was obtained without respecting sufficient safeguards, this automatically renders evidence inadmissible or if there is room for balancing the seriousness of the human rights violation against the relevance of the proof in substantiating charges against persons convicted of international crimes. Both the ICC and the ICTY have taken the view that "the judges have the discretion to seek an appropriate balance between the Statute's fundamental values in each concrete case".[31]

In *Lubanga Dyilo*, the ICC Pre-Trial Chamber argued that, in the fight against impunity, it must ensure an appropriate balance between the rights of the accused and the need to respond to victims' and the international community's expectations. In the light of that, the judges decided that, although "the Items Seized were obtained without regard to the principle of proportionality and in violation of internationally recognised human rights", they should nevertheless be admitted into evidence as a result of the balance made between the seriousness of the violation and the fairness of the trial as a whole.[32] In making this decision, the ICC endorsed the approach taken some years before by the ECtHR. In *Shenk v Swtzerland*, the applicant complained about the use of a recording of his telephone conversations in the context of a criminal proceeding, arguing that the evidence had been obtained unlawfully and in violation of the right to private life. On the premise that questions regarding the rules on evidence admissibility fall outside the scope of its jurisdiction since it is for the State to legislate on

---

surveillance of communications, their interception and the collection of personal data, including mass surveillance, interception and collection, with a view to upholding the right to privacy by ensuring the full and effective implementation of all their obligations under international human rights law".

30 *Ayyash et al*, *op. cit.*, note 12, para. 108.

31 *Brđanin*, *op. cit.*, note 24, where the point was made that "admitting illegally obtained intercepts into evidence does not, in and of itself, necessarily amount to seriously damaging the integrity of the proceedings". (*ibid.*, para. 61); *Prosecutor v Delalić et al.*, Case No. IT-96-21, Decision on the Motion of the Prosecution for the Admissibility of Evidence, 19 January 1998; *Prosecutor v Kordić and Cerkez*, Case No. IT-95-14/2-T, p. 13694, where it is stated that: "[…] evidence obtained by eavesdropping on an enemy's telephone calls during the course of a war is …not antithetical to and certainly would not seriously damage the integrity of the proceedings".
*Lubanga Dyilo, op. cit.,* note 24, para. 74. See in this regard also Zappala, S., *Human Rights in International Criminal Proceedings*, Oxford University Press, Oxford, 2003. According to the author: "The approach adopted so far has been to admit any evidence that may have probative value, unless the admission of such evidence is outweighed by the need to ensure a fair trial" (*ibid.*, p. 149).

32 Lubnga Dyilo, *op. cit.*, note 24, para. 89 ff.

the matter in its discretion, the ECtHR stated that the admission into evidence of unlawfully collected information should not, *per se*, amount to a violation of the right to a fair trial. In order to ascertain whether such violation occurred, it went on, the judges must be satisfied, first, that the defendant did not have the opportunity to challenge the authenticity of the proof and to oppose its use, and, second, "that the recording of the telephone conversation was not the only evidence on which the conviction was based".[33]

In accordance with suggestions coming from human rights bodies, the International criminal tribunals generally favor corroboration of digital evidence through external indicators. External indicators include testimony[34] or information on the identity of the source, sometimes provided by experts, like in the *Ongwen* case, whereas internal indicators consisted of timestamps and metadata.[35] Concerning internal indicators, the ICC adopted an "e-Court Protocol", which provided specific standards of admissibility and reliability of digital evidence. To "ensure authenticity, accuracy, confidentiality and preservation of the record of proceedings", the Protocol requires metadata to be attached, including the chain of custody in chronological order, the identity of the source, the original author and recipient of the information, and the author and recipient's respective organizations. However, as some scholars have correctly pointed out, "while the Protocol offers some guidance to facilitate the use of digital evidence, it is limited to harmonizing the format of digital evidence, and how it is stored in the Court's systems, and does not address issues of probative value of digital evidence",[36] nor the question of its compliance with human rights standards. It is worth noting that the lack of specific rules and guidelines for gauging the admissibility and weight of digital evidence may also impact the possibility for the defendant to contest its use in criminal proceeding and, therefore, bear on their right to a fair trial. This concern is heightened by the fact that defendants in general have limited resources compared with

---

33 *Schenk v Switzerland*, Application No. 10862/84, Judgment, 12 July 1988, para. 48. For a comment on the jurisprudence of the ECtHR in this regard see Quattrocolo, S., *Artificial Intelligence, Computational Modelling and Criminal Proceedings,* Springer, Cham, 2020, pp.73-98; Thake, A. M., *The (In) Admissibility of Unlawfully Obtained Evidence at the International Criminal Court*, Hague Yearbook of International Law: Annuaire De La Haye De Droit International, Vol. 28, 2015, pp. 161-187.

34 See for example *Tolimir* in this regard.

35 On these aspects see *The working paper on "An Overview of the Use of Digital Evidence in International Criminal Courts"*, Salzburg workshop on cyberinvestigations, 2013, [https://humanrights.berkeley.edu/sites/default/files/publications/an-overview-of-the-use-of-digital-evidence-in-international-criminal-courts-salzburg-working-paper.pdf], Accessed 12 January 2023.

36 *Ibid.,* p. 4 ff.

those of the Office of the Prosecutor and may lack the technical ability required to properly challenge digital evidence on the basis of how it was collected.[37]

## 4. CONCLUDING REMARKS

The analysis conducted here illustrates the advantages and opportunities offered by digital technologies in the prosecution of international crimes, especially in the context of proceedings before international courts and tribunals, which, due to their temporal and geographical distance from crime scenes, may be at a disadvantage for fact-finding as compared with domestic courts.

Despite its relevance, however, digital evidence raises significant issues relating to reliability and admissibility. To overcome criticism about admitting evidence collected through information technologies, International criminal tribunals generally tend to require digital evidence to be accompanied by metadata and to be, in the most controversial cases, corroborated by witness testimony. The same approach can be found *a fortiori* in cases where challenges to the admissibility of evidence are grounded on human rights considerations. As the jurisprudence of the ECtHR also shows, the use of technological devices for gathering information may, in fact, raise concerns relating to the right to private life. It is worth noting, however, that not all interferences in the life of individuals necessarily amount to a breach of the right, provided that they are justified by security reasons or that they are necessary to investigate the commission of a crime.

Even in cases where a violation has occurred, this alone is not sufficient to render the evidence inadmissible. In these cases, judges must rather assess the impact on the reliability of the evidence and on the integrity of the proceedings as a whole. This implies that the use of technology for investigation purposes must be evaluated against due process standards. To that end, some scholars suggest that the international criminal tribunals develop specific guidelines and rules to address the digital evidence and to overcome the limits of old procedural guarantees, developed at a time when the use of modern technologies was still highly unusual.[38] Although the ICC has taken some steps in this regard, through the adoption of the "E-court Protocol" and through the appointment of a Scientific Advisory Board to assist the Office of Prosecutor in verifying the authenticity and reliability of the evidence, further efforts must be made to revise procedural rules, in order

---

[37] On this issue and more generally for a recent critical analysis on the relevance of human rights standards of fair trial in the jurisprudence of the ICC, see De Arcos Tejerizo, M., *Digital evidence and fair trial rights at the International Criminal Court,* Leiden Journal of International Law, Vol. 36, No.3, 2023, pp. 749-769.

[38] See Freeman, L., *op. cit.*, note 6, p. 64.

to ensure that the rights of all parties are fully guaranteed.[39] Only in this way will digital evidence, with all its great potential for prosecuting the worst violations of human dignity that amount to international crimes, provide support for the pursuit of justice rather than risk undermining the perception of its fairness and credibility.

## REFERENCES

### BOOKS AND ARTICLES


1. De Arcos Tejerizo, M., *Digital evidence and fair trial rights at the International Criminal Court,* Leiden Journal of International Law, Vol. 36, No.3, 2023, pp. 749-769
2. Freeman, L., *Digital Evidence and War Crimes Prosecutions: The Impact of Digital Technologies on International Criminal Investigations and Trials*, Fordham International Law Journal, Vol. 41, No. 2, 2018, pp. 283-336
3. Freeman, L., *Prosecuting Atrocity Crimes with Open Source Evidence: Lessons from the International Criminal Court*, in: Dubberley, S.; Koenig, A.; Murray, D. (eds.), Digital Witness - Using Open Source Information for Human Rights Investigation, Documentation, and Accountability, Oxford University Press, Oxford, 2019, pp. 48-67
4. Freeman, L.; Vazquez Llorente, R., *Finding the Signal in the Noise: International Criminal Evidence and Procedure in the Digital Age*, Journal of International Criminal Justice, Vol. 19, No. 1, 2021, pp. 163–188
5. Fremuth, M., *Prosecutor v. Ayyash et al (Special Trib. Leb.)*, International Legal Materials, Vol. 60, No. 3, 2021, pp. 357-447
6. Harmon, M.B., *Prosecuting Massive Crimes with Primitive Tools: Three Difficulties Encountered by Prosecutors in International Criminal Proceedings*, Journal of International Criminal Justice, Vol. 2, No. 2, 2004, pp. 403–426
7. Hellwig, K., *The Potential and the Challenges of Digital Evidence in International Criminal Proceedings,* International Criminal Law Review, Vol. 22, No. 5-6, pp. 965-988
8. Land, M.; Aronson, J. (eds.), *New Technologies for Human Rights Law and Practice*, Cambridge University Press, Cambridge, 2018
9. Marchesi, D., *Intercepted Communications in the Ongwen Case: Lessons to Learn on Documentary Evidence at the ICC*, International Criminal Law Review, Vol. 22, No. 5-6, 2022, pp. 920-940
10. Quattrocolo, S., *Artificial Intelligence, Computational Modelling and Criminal Proceedings,* Springer, Cham, 2020
11. Quelling, C., *The Future of Digital Evidence Authentication at the International Criminal Court*, Journal of Public & International Affairs, May 2022.
12. Roscini, M., *Digital Evidence as a Means of Proof before the International Court of Justice*, Journal of Conflict & Security Law, Vol. 21, No. 3, 2016, pp. 541-554


[39] In this vein see Hellwig, K., *The Potential and the Challenges of Digital Evidence in International Criminal Proceedings,* International Criminal Law Review, Vol. 22, No. 5-6, pp. 965-988.

13. Sandalinas, J., *Satellite Imagery and its use as Evidence in the Proceedings of the International Criminal Court*, Zeitschrift Für Luft-Und Weltraumrecht: Vierteljahresschrift Des Instituts Für Luft- Und Weltraumrecht Der Universität Köln, Vol. 64, No. 4, 2015, pp. 666-675
14. Thake, A. M., *The (In)Admissibility of Unlawfully Obtained Evidence at the International Criminal Court*, Hague Yearbook of International Law: Annuaire De La Haye De Droit International, Vol. 28, 2015, pp. 161-187
15. Zappala, S., *Human Rights in International Criminal Proceedings*, Oxford University Press, Oxford, 2003

**ECHR**

1. *Schenk v Switzerland*, Application No. 10862/84, Judgment, 12 July 1988
2. *Amann v Switzerland*, Application No. 27798/95, Judgment, 16 February 2000
3. *Centrum För Rättvisa v Sweden*, Application No. 35252/08, Judgment, 25 May 2021
4. *Big Brother Watch and Others v The United Kingdom*, Applications Nos. 58170/13, 62322/14, 24960/15, Judgment, 25 May 2021
5. *Malone v United Kingdom*, Application No. 8691/79, Judgment, 2 August 1984

**INTERNATIONAL CRIMINAL COURT**

1. *Prosecutor v Al Mahdi*, Case No. ICC-01/12-01/15-171, Decision on the confirmation of charges against Ahmad Al Faqi Al Mahdi, 24 March 2015
2. *Prosecutor v Dominic Ongwen*, Case No. ICC-02/04-01/15, Judgment, 4 February 2021
3. *Prosecutor v Ongwen, Case* No. ICC-02/04-01/15, Public Redacted Version of 'Corrected Version of "Defence Closing Brief", 13 March 2020
4. *Prosecutor v Thomas Lubanga Dyilo*, Case No. ICC-01/04-01/06, Decision on the confirmation of charges, 29 January 2007

**INTERNATIONAL CRIMINAL TRIBUNAL FOR RWANDA**

1. International Criminal Tribunal for Rwanda, Rules of Procedure and Evidence (last amended in 2015, adopted on 29 June 1995)
2. *Prosecutor v Bagosora*, Case No. ICTR-98-41-T, Trial Judgment and Appeals Judgment, 8 December 2008 and 14 December 2011

**INTERNATIONAL CRIMINAL TRIBUNAL FOR THE FORMER YUGOSLAVIA**

1. *Prosecutor v Blagojević and Jokić*, Case No. IT-02-60-T, Decision on the admission into evidence of intercept-related materials, 18 December 2003
2. *Prosecutor v Delalić et al.*, Case No. IT-96-21, Decision on the Motion of the Prosecution for the Admissibility of Evidence, 19 January 1998
3. *Prosecutor v Kordić and Cerkez*, Case No. IT-95-14/2-T

4. *Prosecutor v Popović et al*, Case No. IT-05-88-T, Decision on Admissibility of Intercepted Communications, 7 December 2007
5. *Prosecutor v Radoslav Brdanin*, Case No. IT-99-36-T, Decision on the defence "objection to intercept evidence", 3 October 2003
6. *Prosecutor v Radislav Krstic*, Case No. IT-98-33, Judgement, 2 August 2001
7. *Prosecutor v Tolimir*, Case No. IT-05-88/2-T, Judgment, 12 December 2012
8. International Criminal Tribunal for the former Yugoslavia, Rules of Procedure and Evidence (last amended in 2015, adopted on 11 February 1994)

**SPECIAL TRIBUNAL FOR LEBANON**

1. *Prosecutor v Ayyash et al*, Case No. STL-11-01, Decision on Motions for the Admission of the Call sequence tables related to the five colour-coded mobile telephone groups and networks, 31 October 2016

**UNITED NATIONS**

1. International Commission of Inquiry on Darfur, *Report of the International Commission of Inquiry on Darfur to the United Nations Secretary-General*, 2005, [https://www.legal-tools.org/doc/1480de/pdf/], Accessed 12 January 2023
2. UN General Assembly, Resolution no. 68/167 on the right to privacy in the digital age (A/RES/68/167), 18 December 2013
3. UN Human Rights Committee, General Comment 31, Nature of the General Legal Obligation on State Party to the Covenant (CCPR/C/21/Rev.1/Add 13), 24 May 2004

**REPORTS**

1. European Commission, *European Data Informatics Exchange Framework for Courts and Evidence*, European Evidence Project, available online at [www.cordis.europa.eu/project/id/608185/reporting/de], Accessed 12 January 2022
2. Leiden University, *Report on Digitally Derived Evidence In International Criminal Law*, Part of the digitally derived evidence Project, 2019, [https://leiden-guidelines.com/assets/DDE%20in%20ICL.pdf], Accessed 12 January 2023
3. *The working paper on "An Overview of the Use of Digital Evidence in International Criminal Courts"*, Salzburg workshop on cyberinvestigations, 2013, [https://humanrights.berkeley.edu/sites/default/files/publications/an-overview-of-the-use-of-digital-evidence-in-international-criminal-courts-salzburg-working-paper.pdf], Accessed 12 January 2023