GIURISPRUDENZA PENALE

Open-source information in criminal proceedings: lessons from the International Criminal Court and the Berkeley Protocol.

by ***Stefano Trevisan*** [1]

Summary. Introduction. – **1**. Online open-source information as digital evidence: benefits and challenges. – **2**. Evidence Law governing the International Criminal Court. **3**. Main criteria for evaluating evidence at the International Criminal Court. – **3.1.** Reliability and credibility. – **3.2.** Authenticity. – **4**. International Criminal Court case law on evidence derived from online open-source information. – **4.1.** *Ahmad Al-Faqi Al-Mahdi* Case. – **4.2.** *Bemba et al* Case. – **4.3.** *Al-Werfalli* Case. – **5**. The role of the Berkeley Protocol. – Conclusions.

Introduction.

The Internet contains a seemingly endless supply of information. Estimates are that online storage and service companies like Google, Amazon, and Microsoft hold at least 1,200 petabytes of data, equal to 1.2 million terabytes. As of February 2021, at least 5.18 billion website pages are publicly available online.

The use of social networking sites has proliferated during the last ten years. Facebook, Twitter, Instagram and other platforms have around 3.6 billion users worldwide – figures that are expected to grow. Every minute, over 350,000 tweets are posted on Twitter and over 500 hours of video are uploaded to YouTube.

This immense body of data provides new opportunities across many fields, including within legal practice. Lawyers around the world are increasingly using online open-source information (OSI) to gather evidence that has proved decisive in legal disputes. In criminal proceedings, since the early 1990s, online OSI has revolutionized how human rights violations and international crimes are documented. Social media has become a profoundly powerful tool for first responders, survivors and other actors to communicate what is happening on the ground quickly and effectively. In addition, there is a growing body of content produced by perpetrators themselves who broadcast their crimes for propaganda and recruitment purposes.

[1] LL.M., qualified lawyer and open-source investigator. The author thanks Professor Marco Pertile (Trento University), Aimel Yousfi-Roquencourt (Former ICC assistant legal officer) and Niamh Quille (lawyer at Birnberg Peirce) for their invaluable feedback and peer-review.

As a result, there is now a steady stream of data documenting atrocities, even in the context of armed conflicts. The unprecedented confluence of two technologies – smartphone and social media – has produced, via the instant upload, a new phenomenon: the so called "YouTube war"[2]. For the first time in history, the lengthy war in Syria has been documented with OSI almost in real time.

The expansion of access to the production, dissemination, and collection of OSI has been met with particular interest by the International Criminal Court (ICC), where the Office of the Prosecutor (OTP) investigates grave crimes that generally occur a great distance from The Hague, with little or no judicial assistance nor cooperation provided by the interested State party.

Recently, there has been a significant increase in the use of online OSI at the ICC. Online OSI such as satellite imagery, videos, and geolocation helped lead to the conviction of Ahmad Al-Faqi Al-Mahdi who pleaded guilty to the war crime of destroying cultural property in Timbuktu[3]. In the case against Jean-Pierre Bemba Gombo and members of his legal team for abuses against the administration of justice (i.e. witness tampering), the prosecutor submitted Facebook photographs to evidence the relationship between the parties to an alleged bribery scheme[4]. In 2017 and 2018, the ICC issued an arrest warrant for Libyan Commander Mahmoud Al-Werfalli for thirty-three counts of the war crimes of murder based primarily on execution videos found on social media[5].

The value of OSI cannot be overestimated. But in the era of disinformation, fake news, and alternative facts - which some refer to as the "post-truth era" - this innovative form of evidence is not infallible. The use of OSI in criminal proceedings is capable of leading to violations to the accused's human right to a fair trial.

In order to optimize OSI's potential, investigators and lawyers must consider evidentiary and procedural issues from the start of the investigation in order to ensure its reliability. To assist in this effort, this paper aims to review and discuss whether and to what extent judges have considered the admissibility and probative value of OSI evidence presented in proceedings before the ICC and outlines the most relevant guidelines provided by the recently published Berkeley Protocol.

Part I outlines a definition of online OSI and discusses its major benefits and challenges in criminal proceedings. Part II provides an overview of the evidence rules governing the proceedings at the ICC relevant to this inquiry.

[2] KAYLAN M., "*Syria's war viewed almost in real time*", The Wall Street Journal (2013).

[3] *The Prosecutor v Al Mahdi* (Ahmad Al Faqi), Case no ICC-01/12-01/15.

[4] *The Prosecutor v. Jean-Pierre Bemba Gombo, Aimé Kilolo Musamba, Jean-Jacques Mangenda. Kabongo, Fidèle Babala Wandu and Narcisse Arido*, Case ICC-01/05-01/13-1989-Red.

[5] *The Prosecutor v Mahmoud Mustafa Busayf Al-Werfalli* (Warrant for Arrest), Case ICC-01/11-01/17.

Part III further discusses the approach the ICC has taken thus far to assess OSI and its probative value and evidence weight. Part IV and V examine ICC recent case law using online OSI and explore the most interesting guidelines provided by the Berkeley Protocol. The paper concludes arguing that the ICC is one of the most progressive judicial institutions worldwide to non-traditional investigative approach. However, in criminal proceedings the current enthusiasm for OSI must learn to work within procedural rules, one of the aims of which is to protect the rights of the accused.

1. Online open-source information as digital evidence: benefits and challenges.

OSI is publicly available information that anyone can obtain by request, purchase, or through observation[6]. In other words, it identifies any information that is not 'confidential' and is available in the public domain. Examples of OSI include information available through the media outlets (e.g. radio, television, newspapers, websites, blogs), official reports, academic sources (papers, conferences, seminars), commercial data and so-called 'gray literature' such as working papers, unofficial government documents and surveys. Online OSI is found on the Internet, and may include online news articles, blog-posts or website content; PDF reports and digital documents; social media posts and user-generated content; digital imagery, video and audio recordings; satellite imagery, maps and geospatial data; user data and statistical information; and information contained in Internet archives and database.

OSI may be introduced into court as 'electronic evidence', which is defined as "*data (comprising the output of analogue devices or data in digital form) that is manipulated, stored or communicated by any manufactured device, computer or computer system or transmitted over a communication system*"[7].

The benefits of using OSI in international criminal proceedings are many. Investigators may have limited physical access to the location where the alleged crime took place, due to State refusal to cooperate or safety concerns[8]. OSI can be collected remotely and almost contemporaneously as events take place, and thus it does not threaten investigator security in the context of armed conflicts. OSI is therefore indispensable for finding information, especially in the early stages of investigation.

In addition, OSI is more cost-effective than other forms of evidence collection, such as the taking of witness evidence, and it can also provide

[6] DUBBERLY S., KOENING A, MURRAY D. "*The Emergence of Digital Witnesses*", in "*Digital Witness*", Oxford, (2020).

[7] MASON S., SENG D., "*Electronic Evidence*", University of London, School of Advanced Study, Institute Of Advanced Legal Studies, 4th edition (2017).

[8] LAVING L. "*The Reliability of Open-Source Evidence in the International Criminal Court*", Lund University, (2014).

extra information, which sometimes cannot be gained by human perception, including for example the sunlight incidence angle recorded during a certain event or gunshot acoustic signature. Moreover, it must be taken into consideration that the crimes under the Court's jurisdiction are those of a particular nature – the crime of genocide, crimes against humanity, war crimes and the crime of aggression. Those crimes involve extreme violence, large territories, hundreds of different suspects, victims, witnesses and often also political propaganda against different national, religious, racial or ethnic groups. Because of the special character of those crimes, OSI is capable of overcoming the obstacles inherent in these complex offences, yielding valuable evidence[9].

Notwithstanding this, it should be noted that until recently courts were generally sceptical of evidence derived from the Internet. In a verdict of 1999, a US District Court famously opined[10] that information from the Internet was "*voodoo information*", as "*anyone can put anything on the Internet. No web-site is monitored for accuracy and nothing contained therein is under oath or even sub-ject to independent verification absent underlying documentation* (...) *Moreover, the Court holds no illusions that hackers can adulterate the content on any web-site from any location at any time".* For these reasons, the Court held that online OSI *"is adequate for almost nothing"* in legal proceedings.

Though the approach has changed significantly since then, the use of OSI as evidence in court still raises issues even today, particularly in criminal proceedings. Major criticism derives from the fact that the authors of such OSI information are often unknown or contested. This lack of information on authorship may cast doubt on the independence and impartiality of the original source and may violate the accused's right to cross-examination.

It has been stated that social media creates a dangerous illusion of unmediated information flows[11]. Those who follow YouTube videos, Twitter accounts, or Facebook postings related to the conflict in Syria, Yemen or Libya may believe that they are viewing an accurate and comprehensive account of the events. In reality, these flows are often curated by networks of partisan individuals or organizations who intend to portray particular narratives.

Misattribution staging and technical manipulation are also important pitfalls of online OSI[12]. Misattribution occurs when online content is deliberately or

[9] Ibidem.

[10] US District Court for the Southern District of Texas, *St. Clair v. Johnny's Oyster & Shrimp* - 76 F. Supp. 2d 773 (1999). Cfr. also HONORABLE D. H., YOONJI K. "*Is the Internet "Voodoo"? Evidentiary Weight of Internet-Based Material in Immigration Court*", Connecticut Public Interest Law Journal (2010).

[11] Laving L., id.

[12] MEHANDRU N., KOENIG A., "*Icts, Social Media, & the Future of Human Rights*", Duke Law & Technology Review, pag. 135 (2019).

inadvertently attributed with the wrong date, time, location, or subject. For example, in 2015 a video posted on YouTube purportedly showed "*200 Syrian children being lined up and gunned by ISIS*"[13]. The story was initially published by major UK news websites and quickly spread to other news websites. However, this piece of information was completely untrue. The video was in fact reproducing an incident which had occurred more than a year earlier, where ISIS had executed what was claimed to be over 200 soldiers from Tabqa airbase, near Raqqa, Syria.

Staging transpires when one party attempts to frame another by "staging" and filming an event that never occurred, or edits a video to mislead viewers about what actually took place. Technical manipulation involves manipulating photos and videos with Photoshop or other photo editing tools (e.g., swapping out military insignia). Further, generative adversarial networks are increasingly being used to generate "deep fakes," artificially-generated videos that suggest someone said or did something that in reality never occurred.

Given the vast number of ways OSI can be altered, evidence derived from online OSI must be carefully verified and authenticated, especially when its purpose is to establish criminal liability.

2. Law of evidence governing the International Criminal Court.

To understand this new and vast category of evidence, it is important to consider the concept of evidence and the evidentiary rules surrounding it which are key in criminal proceedings.

Evidence is information submitted to a court by parties to a case with the view of establishing or disproving alleged facts[14]. Evidence introduced in legal proceedings has the potential to make the factual account of either party more or less probable[15].

The law of evidence governs how proceedings will achieve their ultimate purpose, which is to "*verify opposing reconstructive hypotheses of facts"*[16]. In addition, the overriding purpose of evidentiary and procedural rules is to ensure that trials meet fundamental standards of fairness and justice.

[13] HIGGINS E., "*Misattribution, Verification, ISIS, and Madaya*", at www.bellingcat.com (2016).

[14] THE MAX PLANCK ENCYCLOPEDIA OF INTERNATIONAL LAW, "*International Courts and Tribunals, Evidence*" (2013).

[15] MASON S., SENG D., id. Evidence is also famously defined as "*mécanism destiné à établir une convition sur un point incertain*" by LÉVI-BRUHL, "*La preuve judiciarie, Etude de Sociologie Juridique*" (1964).

[16] TARDINO V., "*Il giudizio penale tra fatto e valore giuridico*", pag. 35 in "*La prova penale*", Volume III (2008).

Evidence law ensures that the rights of witnesses, suspects, and the accused are protected through the following of proper procedures[17].
Most textbooks on the law of evidence identify four general categories of evidence: testimonial, documentary, physical, and forensic. Online OSI such as digital photographs, satellite images, digital audio and video-recordings, and other electronic communications or records are considered documentary evidence and are therefore evaluated based on the same criteria as paper documents[18].
Evidence used in criminal cases may fall into two categories: crime-based evidence and linkage evidence. Crime-based evidence is relevant and reliable information about what happened — what offence was committed against whom, when, and where[19]. Crime-based OSI evidence might include footage of, for example, a person being assaulted, property destruction, victim injuries, a mass grave, troops confiscating humanitarian aid, etc. On the other hand, linkage evidence is relevant and reliable information that helps to attribute criminal liability to a specific actor. In other words, it helps prove who committed the crime and how they did it (e.g. individual perpetration, conspiracy, aiding and abetting, or command responsibility). This could include footage of military vehicles, uniforms, patches on uniforms, weapons, military offices, perpetrators training their forces, speeches where the suspect admits she or he was in command of the forces who perpetrated the crime[20].
Evidence can be used for different purposes. 'Lead evidence' points to a crime and allows to make an educated guess about what may have happened. The information alone, however, is not sufficient to determine whether a crime actually happened. 'Prima facie evidence' allows a key fact to be established or presumed true unless it is disproved. 'Corroborative evidence' supports or verifies evidence supporting an assertion. 'Exculpatory evidence' helps prove a defendant is innocent or did not intend to commit a crime[21].
The Rome Statute and the Rules of Procedure and Evidence govern the evidentiary rules of the ICC. Under Art. 69(4) of the Rome Statute, the Court applies a three-step test for determining the admissibility of a piece of evidence. First, the item must be relevant to the case. Secondly, the item must have probative value. Finally, the judges assess whether the relevance and

[17] FREEMAN L., "*Digital Evidence and War Crimes Prosecutions: The Impact of Digital Technologies on International Criminal Investigations and Trials*", Fordham International Law Journal Volume 41, Issue 2, (2018).
[18] FREEMAN L., ibidem.
[19] MATHESON K., "*Video as Evidence Field Guide*", Witness (2016).
[20] Ibidem.
[21] Ibidem.

probative value of the item outweigh any prejudicial effect its admission may cause[22].

In practice though, most evidence is usually admitted, and any questions concerning its relevance, probative value and prejudicial effect is dealt with subsequently during the evaluation phase, when the Court assess the weight to be attributed to the specific piece of evidence[23].

ICC evidence rules do not designate categories of inadmissible evidence. As a consequence, any information derived from the Internet is, in theory, admissible. However, Art. 69(7) of the Rome Statute prohibits evidence acquired by means that violate the Rome Statute or human rights if "*the violation casts substantial doubt*" on the reliability of the evidence or its admission would be "*antithetical*" and would "*seriously damage the integrity of the proceedings*"[24]. This provision is drafted narrowly and does not provide for the automatic exclusion of evidence[25]. Under Art. 69(7), the Court must assess whether the content of the evidence would have been different had the investigation been conducted in full adherence to the Rome Statute or to human rights norms. If the content of the evidence would not change depending on the adherence to the human rights during the collection of evidence, then the violation cannot be serious enough to cast substantial doubt on the reliability of evidence. In this respect, it should be noted that open-source investigators may collect data that are covered by privacy law, including information that relates to an identified or identifiable living individual (i.e. his/her racial or ethnic origin, religious belief or sexual orientation). However, being this is information publicly available online, it is unlikely that the resulting piece of evidence would be excluded on the basis of Art. 69(7). This is because the content of the online OSI is generally not dependent on the way it is obtained[26].

According to ICC case law[27], the burden of proof of the reliability of a document lies on the party seeking its admission. Judges have the authority to "*assess freely*" all evidence submitted in order to determine its relevance

[22] Cfr. Prosecutor v Katanga, Decision on the Prosecutor's Bar Table Motions, 17 December 2010, ICC-01/04-01/07-2635; para 14; and maybe Prosecutor v. Lubanga, Decision on the admissibility of four documents, 13 June 2008, ICC-01/04-01/06-1399 paras. 27.

[23] Cfr. FREEMAN L., "*Prosecuting Atrocity Crimes with Open Source Evidence, Lessons from the International Criminal Court*", pag. 50 in Digital Witness, Oxford (2020); HIATT K., "*Open-Source Evidence on Trial*", The Yale Law Journal, 2016; ASHOURI, A., BOWERS C., WARDEN C. "*An Overview of the Use of Digital Evidence in International Criminal Courts*", Digital Evidence and Electronic Signature Law Review (2014).

[24] The International Criminal Court, Rome Statute Art. 69(7).

[25] ICC-01/04-01/07 Katanga case, Decision on the Prosecutor's Bar Table Motions, para 15.

[26] LAVING L., id pag. 27.

[27] *Prosecutor v. Bemba*, ICC-01/05-01/08-2299, at par. 247.

or admissibility[28] and must "*give reasons for any rulings it makes on evidentiary matters*" (Art. 64(2) Rules of Procedure and Evidence).
In sum, the evidentiary rules of the ICC are particularly flexible and permissive. This legal framework allows the Court to evaluate evidence derived from new technology and devices, such as online OSI.

3. Main criteria for evaluating evidence at the International Criminal Court.

Lawyers, judges and other legal professionals commonly assess the weight of evidence and its probative value by using non-mathematical concepts. In other words, the probative value of evidence is not measured in terms of grams, volts or any other precise physical measure, but rather in terms of probability judgments (for example, I am confident that X is the murderer).[29]
The ICC Chamber famously held that assessing evidence requires an examination of the "*provenance, source or author, as well as their role in the relevant events, the chain of custody from the time of the item's creation until its submission to the Chamber, and any other relevant information*."[30]
Probative value, according to the Court, is determined via a "*fact-specific inquiry [that] . . . take[s] into account innumerable factors, including the indicia of reliability, trustworthiness, accuracy . . . as well as . . . the extent to which the item has been authenticated*."[31]
From the above, it follows that probative value is an overall concept that may involve many factors and we will now discuss these components in turn.

3.1. Reliability and credibility.

The notion of 'reliability' is the quality of being trusted or believed. In its classical meaning reliability refers to dependable and consistent results capable of being obtained by a replicable and repeatable process[32].

---

[28] Cfr. ICC-01/04-01/06 Prosecutor v Lubanga, 16 June 2008, Corrigendum to Decision on the admissibility of four documents, par. 26 "*For these reasons, the Chamber has concluded that it enjoys a significant degree of discretion in considering all types of evidence. This is particularly necessary given the nature of the cases that will come before the ICC: there will be infinitely variable circumstances in which the court will be asked to consider evidence, which will not infrequently have come into existence, or have been compiled or retrieved, in difficult circumstances, such as during particularly egregious instances of armed conflict, when those involved will have been killed or wounded, and the survivors or those affected may be untraceable or unwilling - for credible reasons - to give evidence*".

[29] ANDERSON, T., SCHUM, D., & TWINING, W. "*Analysis of Evidence*", at pag. 228, Cambridge University Press (2005).

[30] *Prosecutor v. Bemba et al*, Judgment at par. 247

[31] *Prosecutor v. Bemba*, ICC-01/05-01/08-2299, Decision on the Prosecution's Application for Admission of Materials into Evidence Pursuant to Art. 64(9) of the Rome Statute, par. 8.

[32] Laving L., id; Cfr. also Berkeley Protocol, page. 8: "*Reliability refers to the ability to perform consistently, dependably or as expected*".

In legal proceedings, reliability is assessed on a case-by-case basis for the purpose of establishing whether a piece of evidence is what it purports to be. If an item of evidence is deemed insufficiently reliable, it can hardly be considered to prove anything.
In the case *Prosecutor v. Germain Katanga And Mathieu Ngudjolo Chui*[33], the ICC Third Chamber laid down the key factors in determining reliability: i) *source* - whether the source of the information is biased; ii) *nature and characteristics* of the item of evidence; iii) *contemporaneousness* - whether the information was obtained and recorded simultaneously or shortly after the events to which it pertains or whether the record was created at a later stage; iv) *purpose* - whether the document was created for the specific purpose of these criminal proceedings or for some other reason; and e) *adequate means of evaluation* - whether the information and the way in which it was gathered can be independently verified or tested.
In sum, the evaluation of reliability involves the general trustworthiness of the source of the evidence, having regards both to the "track record" of the source and the methods by which the information was collected.
By contrast, 'credibility' indicates whether what the piece of evidence claims should be believed or not. Credibility, unlike reliability, is something which is judged 'in the moment' during the trial, and pertains to the quality of the information[34]. It involves accuracy, consistency (both internal and external) and clarity of description of the events.

3.2. Authenticity.
Evidence is deemed authentic when is genuine and not forged. Authenticity and reliability are related, but distinct concepts. The purpose of authentication is to ensure that the evidence has not been manipulated or tampered with, while the purpose of reliability is to establish whether a piece of evidence is what it purports to be.
For a physical document, its authenticity comprises such attributes as being faithful to an original, uncorrupted and with a verified provenance (encompassing the following attributes: uniqueness, unambiguity, conciseness, repeatability and comprehensibility)[35]. The rules of evidence that have developed with respect to documentary evidence are also applicable to OSI.

[33] *Prosecutor v. Germain Katanga And Mathieu Ngudjolo Chui,* Case ICC-01/04-01/07, Decision on the Prosecutor's Bar Table Motions.
[34] In *Kunarac et al.*, the ICTY Trials Chamber defined the reliability by comparing it to credibility in the following way: "*Credibility depends upon whether the witness should be believed. Reliability assumes that the witness is speaking the truth, but depends upon whether the evidence, if accepted, proves the fact to which it is directed*", Kunarac et al., TC, 3 July 2000, para 7.
[35] MASON S., SENG D., id.

Authenticity refers to the ability to demonstrate that an electronic item remains unchanged from when it was collected. Courts are particularly concerned with the authentication of electronic evidence such as OSI, because they can be easily manipulated. For example, video footage may be altered or the metadata (internal digital information that describes characteristics of the data) may be changed.
By testing the authenticity of OSI, the court may assess its integrity and provenance. Integrity refers to the "wholeness and soundness" of electronic evidence, and implies that the evidence is complete and unaltered. Maintaining and verifying the integrity of digital evidence items are important technical considerations that could significantly impact their admissibility. Digital data is altered, modified or copied from one environment to another either through human actions or uncontrolled computing activities. Forensic examiners adopt various methods for maintaining and demonstrating the integrity of digital evidence[36]. The use of a write blocker, for example, is a standard digital forensic requirement to maintain the integrity of evidence. Digital signatures, encryption and hash algorithms[37] are also employed to maintain, validate and demonstrate the integrity of digital evidence.
Provenance can be established through a chain of custody, which is defined as "*the movement and location of real evidence, and the history of those persons who had it in their custody, from the time it is obtained to the time it is presented in court*"[38]. Establishing provenance requires both testimony of continuous possession and testimony that the object remained in substantially the same condition during each individual's possession. This information provides a complete history of hosting and possession of who controlled the electronic information, which is important in determining whether evidence has been modified or tampered with when the court assesses the accuracy of the digital evidence.
A strong chain of custody increases the weight judges accord to the evidence because "*factors such as ... proof of authorship will naturally assume the greatest importance in the Trial Chamber's assessment of the weight to be attached to individual pieces of evidence*"[39].

[36] ANTWI-BOASIAKO A., VENTER H., "*A Model for Digital Evidence Admissibility Assessment*", 13th IFIP International Conference on Digital Forensics, DigitalForensics (2017).
[37] BERKELEY PROTOCOL, pag. 60 "*Hash values are a unique form of digital identification that confirm, through the use of cryptography, that the content collected is unique and has not been modified since the time of collection. At the point of collection, open-source investigators should manually add – or the collection tool should automatically add – a hash value*".
[38] ASHOURI, A., BOWERS C., WARDEN C, id.
[39] *Prosecutor v. Brdanin and Talic*, Case No. IT-99-36-T, Order on the Standards Governing the Admission of Evidence, para. 18 (Int'l Crim. Trib. for the Former Yugoslavia, Feb. 15, 2002).

The lack of testimony by an author will not usually preclude the admission of evidence. According to the ICC case law "*nothing in the Statute or the Rules expressly states that the absence of information about the chain of custody ... affects the admissibility or probative value of Prosecution evidence*"[40].
The ICC practice reflects special attention to the authenticity of electronic evidence. When introduced in the proceeding, such evidence must conform to an "e-court Protocol," which is designed to "*ensure authenticity, accuracy, confidentiality and preservation of the record of proceedings*"[41]. 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 information, and the author and recipient's respective organizations. 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.

4. International Criminal Court case law on evidence derived from online open-source information.

In three recent cases the Court laid down "*unique and precedent-setting*"[42] decisions with regard to the use of online OSI. Some guidelines may be drawn from these cases, as illustrated below.

4.1. *Ahmad Al-Faqi Al-Mahdi* Case.

While some online OSI content had already been used in earlier international criminal cases, the conviction of Al-Mahdi has been considered the "*first big test*"[43] of what can be achieved with non-traditional investigative techniques. The accused was an alleged member of the armed group Ansar Dine, who was charged with participating in the intentional destruction of nine mausoleums and the door to a mosque in Timbuktu in 2012. During the proceedings the OPT successfully partnered with open-source investigators and civil society groups to bring evidence into Court. The research agency, Situ, delivered an interactive digital platform[44] designed to facilitate the organization, analysis, and presentation of OSI evidence. Combining geospatial information, historic satellite imagery, photographs, open-source videos, the tool was used to walk the judges and other court actors through

[40] *Prosecutor v. Lubanga*, Case No. ICC-01/04-01/06, Decision on Confirmation Charges, para. 96.
[41] International Criminal Court, "*Unified Technical protocol ("E-court Protocol") for the provision of evidence, witness and victims information in electronic form*", par. 1 (2019 edition).
[42] FREEMAN L, id. pag. 290.
[43] KOENING A., "*Open-source evidence and human rights cases*", in "Digital Witness", pag. 36 (2020).
[44] Cfr. https://situ.nyc/research/projects/icc-digital-platform-timbuktu-mali.

the various events in Timbuktu. In August 2016, at the start of the trial, Al-Mahdi admitted guilt, and he was sentenced to nine years to jail.
Some have criticized the defence choice not to challenge the admissibility of OSI at trial. According to these critics, Google Earth images are not made for the courtroom and their reliability should be thoroughly tested[45]. In any case, the Al-Mahdi investigative approach is notable as it supported civil society and the OPT to understand how online OSI can be sourced, verified, analysed, and presented in ways that can advance legal accountability[46].

4.2. *Bemba et al* Case.
In *Bemba et al* the defendants are the first to be charged with offenses against the administration of justice for interfering with witnesses in another ICC trial, pursuant to Art. 70 of the Rome Statute. The Prosecutor submitted four photographs extracted from the Facebook pages of a defence witness and a prosecution witness to show the relationship between the parties to the alleged bribery scheme. The defence challenged the admissibility of such online OSI, arguing they were not prima facie authentic nor reliable. The defence claimed that it was *"impossible to forensically ascertain, even on a prima facie basis, that a Facebook account under a certain name is attributable to a person of the same name,* [as] *the creation of a Facebook account does not require any valid identity information*"[47]. In addition, the defence contested that the Facebook photographs were genuine, as the Prosecutor had submitted "*merely screenshots of a webpage with a pop-up photograph*", deprived of the "*metadata of the photograph, such as the creation date, the photographing device and the modification traces*"[48]. In the final judgment, the Chamber found all the five accused guilty, although the challenges raised by the defence were not specifically addressed.
In addition, in the related proceeding against Bemba the Chamber reiterated its flexible approach to authenticity of digital evidence by affirming that "*recordings that have not been authenticated in court can still be admitted, as*

[45] Cfr. Freeman L., id. pag. 318: "*The Prosecution was not required to take the additional step of seeking out the raw images from Google, question employees of Google Earth about their process, or verify on the ground the accuracy of the satellites used by Google Earth in that location and time. This is problematic because Google Earth positional accuracy is not fixed but varies from one time to another. […] The reliability of Google Earth images and the extracted positional data should be supported with field checks of the locations and corroborated with other evidence. Additionally, it would be best practice to acquire the original images directly from the source rather than taking screenshots because it is more reliable to uncover potential tampering with the primary image file".*
[46] KOENING A., id. pag. 40.
[47] *Prosecutor v. Bemba et al*, Case ICC-01/05-01/13, Public Redacted Version of Defence Response to Prosecution's Third Request for the admission of Evidence from the Bar Table, par. 84.
[48] Id, par. 85.

in court authentication is but one factor for the Chamber to consider when determining an item's authenticity and probative value."[49] Notably, the judges also admitted as evidence online OSI such as NGO reports. The majority found that they can be considered reliable "*provided that they offer sufficient guarantees of impartiality*" and are therefore admissible "*for the limited purpose that the information contained therein may serve to corroborate other pieces of evidence*"[50].

4.3. *Al-Werfalli* Case.

In August 2017, the Pre-Trial Chamber I of the ICC issued an arrest warrant for Mahmoud Al-Werfalli[51], the commander of al-Saiqa, an elite unit within the Libyan National Army. Al-Werfalli was accused of arbitrarily executing thirty-three people in a series of acts captured in a video uploaded to Facebook. This key online OSI evidence depicts 18 individuals wearing orange jumpsuits and black hoods, with their hands tied behind their backs, kneeling barefooted on the ground in four lines. After reading a "Decree decision", five men in camouflage uniform shot at the kneeling persons.
A few weeks after the issue of the arrest warrant, investigators at Bellingcat reportedly geolocated the execution area (32.023144, 20.029181) by using open-source intelligence tools. Satellite's imagery seems to confirm the location - fifteen black spots are distinctly visible in the image, which are considered to very likely be blood stains of the executed people[52].
Legal and human rights communities hailed the warrant as a milestone, marking the first time the ICC had cited abundant online OSI as a basis for a warrant[53]. For the first time the OPT put online OSI at the heart of an investigation: without the video content, there would have been no case.

5. The role of the Berkeley Protocol.

When resolving the issue of probative value and weight of online OSI evidence, the Chamber assess whether the information and the way in which it was gathered can be independently verified or tested.

---

[49] *Prosecutor v. Jean-Pierre Bemba Gombo*, Case No. ICC-01/05-01/08, Decision on the Prosecution's Application for Admission of Materials into Evidence Pursuant to Article 64(9) of the Rome Statute, para. 120 (Oct. 8, 2012)

[50] Id, Par. 270. In disagreement with the majority's admission of the reports from the International Federation of Human Rights, Amnesty International, and the BBC, Judge Ozaki stated: "*The source of information relied on in the reports are not revealed with sufficient detail, and as a result it is not possible to fully investigate their reliability. Due to lack of guarantees concerning the reliability of these reports' sources, in my judgment the probative value of the three reports is low".*

[51] *Prosecutor v. Mahmoud Mustafa Busayf Al-Werfalli*, Warran of Arrest, ICC-01/11-01/17-2.

[52] Cfr. Bellingcat at https://www.bellingcat.com/news/mena/2017/10/03/how-an-execution-site-was-geolocated/

[53] KOENIG A., id., pag. 40.

Verification is a "*technical term for the process of establishing the reliability or veracity of information - in other words, establishing whether a claim or assertion is true*"[54]. However, there are no binding legal standards that govern the verification process, and authoritative international guidelines have been absent until recently.

Only on 1 December 2020, a collaboration between the Office of the United Nations High Commissioner for Human Rights, and the Human Rights Center at the University of California, Berkeley, School of Law launched the Berkeley Protocol, described as the "*first global guidelines for using publicly available information online – including photos, videos and other content posted to social media sites – as evidence in international criminal and human rights investigations*"[55].

The Protocol avoids tool-specific rules, and instead offers useful guidelines for ensuring that online OSI can be used to meet the required evidentiary threshold in legal proceedings. To ensure authenticity and reliability, the Protocol lays down practical guidelines for collecting, preserving and verifying online OSI. As a minimum standard for providing evidence in court, lawyers and investigators should gain possession of online content by collecting a number of key elements, including the uniform resource locator (URL) and the Hypertext Markup Language (HTML) source, full-page capture, embedded media files and metadata[56]. It recommends the generation of a hash value and for a chain of custody to be maintained during the process. Verification is broken down into three separate considerations: the source, the digital item or file, and the content, which should be looked at collectively. With respect to the latter, the Protocol refers to geolocation and chronolocation techniques to identify the probable location and time of the events depicted by OSI[57].

While the analysis of the specific guidelines outlined is beyond the scope of the present contribution, it should be noted that the Protocol holds that the determination of weight implies an "*holistic assessment*" that depends, in part, on the other information that may support, corroborate or contradict the fact in question[58]. Therefore, external corroboration is key, as it can provide information that lies outside an OSI item and that can "*support the veracity of the item's content*"[59]. An example of such external corroboration may include the witness testimony of the investigators who collected or verified the online OSI submitted to the court, who might be asked to explain the investigative approach, methods and tools used – in other words, whether the open-

[54] DUBBERLY S., KOENING A., MURRAY D., id. pag. 9.
[55] Cfr. https://matrix.berkeley.edu/research/berkeley-protocol-open-source-investigations.
[56] BERKELEY PROTOCOL, pag. 59.
[57] Id., pag. 66.
[58] Id., pag. 26.
[59] Id., pag. 66.

source investigation had complied with the Berkeley Protocol during the investigation[60].

Conclusions.

The Internet is a vast field rich of useful information. With a click of a mouse, seemingly endless content is quickly available, including YouTube videos, social media and satellites images. Both victims and perpetrators increasingly document online grave crimes such as torture, arbitrary execution and violent repression of peaceful protests, almost in real time.

The expansion of OSI has arguably democratized information production and usage, and civil society groups have emerged as an agent in both intelligence gathering and information generation. Investigative platforms like Bellingcat and Lighthouse Reports heavily rely on online OSI, and their investigations have been presented to national and international legislatures, up to the UN level. An ever-increasing number of human rights activists, investigative journalists and lawyers are being trained in how to locate, capture, preserve, verify, and present OSI content for the purpose of achieving legal accountability.

The ICC has proved to be one of the most progressive judicial institution to employ non-traditional investigative approach. The convictions of Bemba and Ahmad Al-Faqi Al-Mahdi, together with the arrest warrant issued against Al-Werfalli clearly showed how OSI can be considered reliable and authentic. However, in criminal proceedings the current enthusiasm for open-source investigation must accord with procedural rules, whose ultimate aim is to protect the fundamental rights of the accused. In adversarial proceedings the truth is arguably more likely to emerge from the open contest between the prosecution and the defence in presenting the evidence and opposing one another's legal arguments. Through the process of argument and counter-argument, examination-in-chief and cross-examination, each side tests the relevancy, reliability and authenticity of the opponent's evidence and arguments. To maintain fairness, there is a presumption of innocence, and the burden of proof lies with the prosecution.

Evidence derived from online OSI is not in any way exempt from criminal procedural rules. The probative value of OSI should be evaluated in the same way as other types of evidence, and their proper introduction in legal proceedings cannot be disadvantageous to the accused. The defence must

[60] Id. pag. 72: "*If the findings of an open source investigation reach a courtroom, investigators might have to testify as witnesses in the case of legal proceedings, it is often the heads of investigations who will have to testify, and they should be able to speak about the work of their teams. That requires, of course, that they know what their teams have done and can answer questions about the roles performed and the reasoning underlying any decision-making concerning the scope of an investigation, its methods, the tools used etc. Investigators may be either expert witnesses or lay witnesses*".

have the opportunity to challenge the process of its creation, chain of custody and content. Experts may also be required to explain what information this newer form of evidence can and cannot provide, especially with unfamiliar and complex technologies. Verification skills are highly demanded.

Bibliography

ANDERSON T., SCHUM D., TWINING W. "*Analysis of Evidence*", Cambridge University Press (2005)

ANTWI-BOASIAKO A., VENTER H., "*A Model for Digital Evidence Admissibility Assessment*", 13th IFIP International Conference on Digital Forensics, in Digital Forensics (2017)

ASHOURI, A., BOWERS C., WARDEN C. "*An Overview of the Use of Digital Evidence in International Criminal Courts*", Digital Evidence and Electronic Signature Law Review (2014)

DE BUSSER E. "*Open Source Data and Criminal Investigations: Anything You Publish Can and Will Be Used Against You*", Groningen Journal of International Law, vol 2(2): Privacy in International Law (2014)

DUBBERLY S., KOENING A, MURRAY D. "*The Emergence of Digital Witnesses*", in "Digital Witness", Oxford (2020)

FREDESVINDA I., "The Admissibility of Electronic Evidence in Court (A.E.E.C.): Fighting against High-Tech Crime—Results of a European Study", Journal of Digital Forensic Practice (2007)

FREEMAN L., "*Digital Evidence and War Crimes Prosecutions: The Impact of Digital Technologies on International Criminal Investigations and Trials*", Fordham International Law Journal Volume 41, Issue 2 (2018)

HIATT K., "Open-Source Evidence on Trial", The Yale Law Journal (2016)

HIGGINS E., "*Misattribution, Verification, ISIS, and Madaya*", Bellingcat (2016),

INTERNATIONAL BAR ASSOCIATION, "Evidence Matters in ICC Trials" (2016)

KOENIG A., MCMAHON F., MEHANDRU N., BHATTACHARJEE S., "*Open-Source Fact-Finding in Preliminary Examinations*", in Morten Bergsmo and Carsten Stahn, eds. Quality Control in Preliminary Examination, vol. 2 (2018)

KOENING A., "*Open-source evidence and human rights cases*", in Digital Witness (2020)

Laving L. "*The Reliability of Open-Source Evidence In the International Criminal Court*", Lund University (2014)

MASON S., SENG D., "Electronic Evidence" 4th edition (2017)

MEHANDRU N., KOENIG A., "*Icts, Social Media, & the Future of Human Rights*", Duke Law & Technology Review 129-145 (2019)

MEHANDRU N., KOENIG A., "*Open-Source Evidence and the International Criminal Court*", Harward Human Rights Journal (2019)

TARDINO V., "*Il giudizio penale tra fatto e valore giuridico*", in La prova penale, Volume III, (2008)