THE APPLICABLE INTERNATIONAL LEGAL FRAMEWORK AND STANDARDS CONCERNING OPEN-SOURCE AND ELECTRONIC EVIDENCE: THE EUROPEAN CONVENTION ON HUMAN RIGHTS

Jeremy McBride*

The use of open-source evidence is already proving useful in proceedings before the International Criminal Court and in some national courts.[1]

In my remarks, I would like to focus first on the practice so far of the European Court of Human Rights regarding the reliance on open source and electronic evidence in proceedings before it and then review the considerations that it has regarded, or is likely to regard, as relevant to possible disputes about the admissibility of such evidence.

In fact, specific reference to the concept of open source material as a form of evidence has barely featured in proceedings before the European Court. In particular, such evidence – as opposed to electronic evidence more generally - has not yet been specifically discussed from the perspective of its admissibility.

Nonetheless, there are certainly cases before the European Court in which social media and messaging systems – which can provide evidence falling into the open source category - have been relied upon by States when seeking to justify actions said by applicants to violate their human rights.

Such claims have not so far succeeded but that has been on account of its content rather than its form.

Thus, the European Court has not been persuaded that evidence based on social media and messaging systems was capable of supporting claims that a person's detention was justified because there was a reasonable suspicion that s/he had committed an offence either because it was insufficient to substantiate such a suspicion (as, e.g., in *Selahattin Demirtaş v. Turkey (no. 2)* [GC], no. 14305/17, 22 December 2020 or was only available to the authorities after it had already taken the decision concerned (as in, e.g., *Baş v. Turkey*, no. 66448/17, 3 March 2020).

Moreover, it has also rejected submissions in, e.g., *Üçdağ v. Turkey*, no. 23314/19, 31 August 2021, that there was insufficient explanation as to why the content of a person's

* Barrister, Monckton Chambers, London and International Consultant of the Council of Europe.

[1] See, e.g., *The Prosecutor v. Ahmad Al Faqi Al Mahdi* (ICC-01/12-01/15).

Facebook page should be interpreted as glorifying, legitimizing and encouraging the methods of coercion, violence and threat employed by the PKK.

In none of these cases, however, was there any suggestion that it would have been inappropriate, as a matter of principle, for national courts to rely on evidence derived from social media and messaging systems.

Furthermore, the European Court has itself relied upon certain forms of evidence of an open source nature, including some that is in a digital form, for the purpose of establishing the facts in cases that have come before it.

Thus, it has relied upon reports prepared by the European Committee for the Prevention of Torture and Inhuman or Degrading Treatment or Punishment such as in, e.g., *Strazimiri v. Albania*, no. 34602/16, 21 January 2020 to support a finding that there was an insufficient level of psychiatric care and the "impression of therapeutic abandonment" of many psychiatric patients which amounted to inhuman and degrading treatment contrary to Article 3 of the European Convention.

It has also relied upon reports of non-governmental organisations when determining cases about the efficacy of judicial control over the detention of migrants and asylum-seekers and the risk of being subjected to inhuman and degrading treatment if a person was removed to a particular country as in, respectively, *Monir Lotfy v. Cyprus*, no. 37139/13, 29 June 2021 and *S.H. v. United Kingdom*, no. 19956/06, 15 June 2010.

In addition, in *Georgia v. Russia (II)*, [GC], no. 38263/08, 21 January 2021, the European Court has referred to the report "High-Resolution Satellite Imagery and the Conflict in South Ossetia" published by the American Association for the Advancement of Science (AAAS), finding that the satellite imagery analysis in the report constituted objective evidence relevant to the issues to be determined in that case and, in particular, the cause of damage to houses in Georgia.

Moreover, the European Court currently has before it links to digital data concerning the location, types and even identity of equipment that might be relevant to the responsibility for the destruction of Malaysian Airlines flight MH117 being considered in communicated case *Ayley and Others v. Russia*, no. 25714/16.

Also, there are many cases where electronic or digital evidence – not of an open source character - has been found to be relevant to establishing claims that particular action by the authorities was in violation of Convention rights and freedoms, such as the use in *Navalnyy*

and Gunko v. Russia, no. 75186/12, 10 November 2020 of a video-recording to show that manner of restraining the first applicant was not indispensable for bringing him to the police station.

Moreover, there are also cases where such evidence was considered to have been properly used as the basis for a person's conviction, such as in:

- *Khodorkovskiy and Lebedev v. Russia*, no. 11082/06, 25 July 2013, in which it was found that nothing in the process of seizing and examining computer hard drives had made the information obtained from them unfit for use at the trial of the applicants;
- *Rook v. Germany*, no. 1586/15, 25 July 2019 where the issue was about simply the extent to which the applicant had sufficient access to text and multimedia messages used against him before the trial and not the use of them at the trial; and
- *Svetina v. Slovenia*, no. 38059/13, 22 May 2018 in which it was found that the use in criminal proceedings against the applicant of data concerning his mobile telephone record had not violated his right to a fair trial.

The European Court has also recognised that geolocation data can be relevant in criminal proceedings to establish a person's presence in a particular place, albeit that access to it was considered in *Sedletska v. Ukraine*, no. 42634/18, 1 April 2021, not to be justified in respect of a journalist who was not the object of the investigation concerned.

The acceptance by the European Court of reliance on open source and electronic evidence, whether in proceedings before it or in ones in national courts, should not be a surprise given its general approach to evidence.

Thus, no rules as to admissibility of evidence or the form that this takes are prescribed in the European Convention. As a result, the European Court regards these as issues as primarily one for regulation under national law, something that it made clear in *Schenk v. Switzerland* [P], no. 10862/84, 12 July 1988 and many subsequent cases. Its concern is rather with the question of whether the proceedings as a whole, including the way in which the evidence was obtained, can be regarded as fair.

Moreover, the mere fact that evidence has been obtained illegally – even if thereby in violation of certain rights under the European Convention - will not lead to the proceedings being considered unfair, as can be seen in *Parris v. Cyprus* (dec.), 56354/00, 4 July 2002 with regard to a post-mortem carried out illegally and in *Khan v. United Kingdom*, no. 35394/97, 12 May 2000 with regard to the use of a covert listening device.

Rather, the concern in such instances will be whether the rights of the defence have been respected and the strength of the evidence, especially where there are no doubts as to its authenticity or reliability.

Although, as has already been mentioned, this is not something that has been a particular concern so far with open source evidence, there is no reason to expect that the European Court will take a different approach to such evidence, albeit that the character of it could make the issue of reliability or authenticity a more significant issue than seen in many of the cases where it has been dealing with digital evidence that is not of an open source character.

One issue that could be relevant in making an assessment about authenticity or reliability of open source evidence could be its provenance.

In this connection, it should be noted the satellite imagery analysis referred to in - which was considered by the European Court to constitute objective evidence – was that the report was produced by the Geospatial Technologies Project as part of the Scientific Responsibility, Human Rights and Law Program of the American Association for the Advancement of Science. It put some emphasis on the fact that this association was a non-profit organisation with the aim of promoting the advancement of science throughout the world and one of the oldest, and perhaps the largest, federations of scientific bodies.

This origin could not be an absolute guarantee of authenticity or reliability but evidence coming from such a body could give some confidence in this regard, certainly more so than evidence from entities that do not have the same track record of methodological rigour.

Also important will be the procedure followed in gathering the open source evidence, something about which the European Court has already been concerned with in the use of evidence supposed obtained through forensic examinations and searches.

Thus, in *Horvatić v. Croatia*, no. 36044/09, 17 October 2013, there was no record on the procedure in accordance with which the applicant's samples were taken and packed for forensic analysis, including as to whether a new pair of gloves had been used each time a different item had been packed. As a result, the lack of any action by the trial court to examine objections as to the manner in which the forensic evidence was obtained and packed during the investigation was considered to have created such a procedural disadvantage to the applicant's detriment that the proceedings as a whole fell short of the requirements of a fair trial.

Similarly, in *Sakit Zahidov v. Azerbaijan*, no. 51164/07, 12 November 2015, the European Court considered that the quality of the physical evidence – drugs allegedly found in the applicant's pocket during a search - on which the domestic courts' guilty verdict was based was questionable because the manner in which it was obtained cast doubt on its reliability.

In that case, the police had failed to conduct a search immediately following an arrest without good reason and the time lapse of around twenty minutes between the arrest and search was seen as raising legitimate concerns about the possible "planting" of the evidence, because the applicant was completely under the control of the police during that time.

Moreover, there is nothing to suggest that there were any special circumstances rendering it impossible to carry out a search immediately after the arrest. Moreover, the arrest was not immediately documented by the police, with the official record only being drawn up almost four hours later.

This underlines the importance of having a clear procedure to be followed when gathering open source digital evidence, including the documentation of the way in which this takes place, and of ensuring that this procedure has been followed and can be demonstrated.

In addition, it will be important to be able to demonstrate that there is no reason to doubt the authenticity of the open source material on account, for example, of it having been fabricated or in some way altered so as to create apparently incriminating evidence.

This is something that the European Court has been faced with already in the case of surveillance operations where, for example, it has been suggested that the recordings of conversations have been manipulated in some way.

For example, in *Văduva v. Romania*, no. 27781/06, 25 February 2014, doubts had been raised about the transcript of a conversation in a prison cell that had been covertly recorded but it had not been possible to get an expert examination of the audio-tapes on which the transcript was claimed to be based. The absence of such an examination was an important consideration for the finding by the European Court that the proceedings against the applicant had not been fair.

It is thus of fundamental importance that a defendant be given a real opportunity to challenge the reliability or authenticity of open source material.

However, more than that it is important that the relevant court deals appropriately with any objections that have been raised. This did not occur, for example, in *Sakit Zahidov v. Azerbaijan*, in which the domestic courts were found to have contented themselves with noting that the applicant's assertion that the evidence against him had been planted was defensive in nature and was not confirmed without actually examining his specific complaints. Since those complaints were thus not considered without any reason being given, the European Court concluded that the applicant had not been given the opportunity to raise this issue.

It will always be an issue where open source material is invoked that it be capable of supporting the finding reached by the court concerned and the European Court will thus scrutinise this closely. A good example of unjustified reliance on a video-recording can be seen in *Dan v. Republic of Moldova (No. 2)*, no. 57575/14, 10 November 2020, in which this related to the alleged taking of a bribe.

The video apparently only captured the moment when the money had been marked with a special powder and the moment when the applicant had been apprehended. However, the moment when the money had been handed over had not been filmed for technical reasons. Not only was the video not actually available at the trial but the absence from it of the crucial moment – the passing of the money - was seen by the European Court to have exacerbated the deficiencies in the overall assessment of the evidence in that case.

Where the authenticity of digital evidence is not in question, the European Court may reach the conclusion – as it did in *López Ribalda and Others v. Spain*, no. 1874/13, 17 October 2019 of the footage recorded by means of video-surveillance of thefts committed by supermarket employees – that this could constitute sound evidence which does not necessarily need to be corroborated by other material.

However, despite saying that, the European Court did note in that case that the recordings in question were not the only evidence on which the domestic courts based their findings since they also took account of the applicants' statements, the testimony of other persons and an expert's report comparing the images recorded by the video-surveillance and the till receipts.

This might point to some hesitation in relying on a limited piece of digital evidence and the availability of corroborative evidence – whether of the same or another form – might be

considered as preferable when assessing whether the reliance on that piece of digital evidence did not undermine the fairness of the proceedings in the case.

The usefulness of open source material as evidence will often depend upon its interpretation, for which the assistance of experts may be crucial. This was evident in *Georgia v. Russia (II)*, in which an expert from the American Association for the Advancement of Science explained that a burnt house looked very different to a bombed house on satellite image, a point of importance in concluding that the satellite images in the Association's report was evidence showing that the majority of the damage to houses in Georgian villages after 10 August 2008 had been caused by burning.

This is not, of course, problematic but, as the European Court has underlined, it may be hard to challenge a report by an expert without the assistance of another expert in the relevant field. Moreover, this may require such an expert to have access to the open source material concerned. Without this and the consequent refusal to consider submissions from an expert called by the defence, the European Court may find, as it did in *Khodorkovskiy and Lebedev v. Russia*, that a disbalance was thereby created between the defence and the prosecution in the area of collecting and adducing "expert evidence", thus breaching the equality of arms between the parties, contrary to Article(1) and(3)(d) on that account.

Finally, although material in social media accounts may not generally be sufficient to sustain a conviction by themselves or to a significant extent, it should be borne in mind that such material might be regarded by the European Court as in effect the testimony of a witness. Certainly, such an approach seems possible in the light of its readiness in *Arlewin v. Sweden* (dec.), no. 32814/11, 2 February 2016 to proceed on the basis that anonymous persons who had made statements in a television programme shown in the course of a trial should be considered as witnesses.

In the event of material from the social media accounts of one or more persons being similarly treated and those persons do not give evidence in person, there would then be a need to take account of the requirements elaborated in *Schatschaschwili v. Germany* [GC], no. 9154/10, 15 December 2015 and subsequent cases, namely, that there be a good reason for their non-attendance and there are sufficient counterbalancing factors to compensate for the handicaps under which the defence would labour in the event of the evidence of those witnesses being the sole or decisive basis for a conviction.

The European Court has not yet had to consider the *Berkeley Protocol on Digital Open Source Investigations* that was developed in collaboration between the Office of the United Nations High Commissioner for Human Rights and the Human Rights Center at the University of California, Berkeley. However, the practical guidelines in it for collecting, preserving and verifying online open source information chime with the more general concern of the European Court that the proceedings as a whole, including the way in which the evidence was obtained, should be regarded as fair. Reliance on these guidelines and, in particular, an ability to demonstrate that this has occurred, is thus likely to lead the European Court to conclude that the fairness of criminal proceedings should not be regarded as having been compromised through the reliance placed by national courts on online open source information, so long as the other considerations relevant for fairness have also been observed.