Evidentiary Matters in the Context of Investigating and Prosecuting International Crimes in Sweden: Admissibility, Digital Evidence and Judicial Notice

Mark Klamberg

1 Principles of Flexible Admissibility and Free Evaluation of Evidence in Swedish Law 368

2 Comparative Outlook on Admissibility and Evaluation of Evidence 370

2.1 Use of Digital Evidence, Smartphone Recordings and Social Media by International Courts and Domestic Courts 372

2.2 Comparative Outlook on Judicial Notice of Facts of Common Knowledge and Adjudicated Facts 375

3 Review of Swedish Case Law 376

3.1 Digital Evidence, Smartphones, Open Sources and Social Media in Swedish Courts 376

3.2 The Use of Facts of Common Knowledge and Adjudicated Facts before Swedish Courts 379

4 Analysis 380

The prosecution of international crimes may entail additional challenges in relation to evidentiary matters. The relevant trials in Sweden have all concerned acts committed outside Sweden in areas of conflict. The consequence is that part of the evidence was collected by other actors than the regular administration of justice, often without the required decisions by a court or other state agency. In addition to questions of whether the collection of evidence follows legal requirements, there will be questions on how the evidence has been handled and stored, i.e. issues related to the chain of custody, which may affect how the authenticity and reliability of the evidence will be assessed.[1] This article examines potential similarities and differences regarding admissibility of evidence and evaluation of evidence, in particular the challenges and opportunities that come with technological development. There will also be an account of how facts of common knowledge and adjudicated facts may be used.

With technological development new tools will continuously appear that may change the character and availability of evidence. When prosecuting international crimes, digital evidence – which includes wire-tapping and surveillance of communication, photos and smartphone videos, open sources and social media sometimes stored on USB flash drives, SD cards, CD, DVD or tape – become particularly relevant. In investigations into international crimes committed on another state's territory, police and prosecutors often have little or no access to the site of the crime and witnesses. Digital evidence may partly compensate for such difficulties. Thus, the question arises of whether digital information can be used as evidence.

As already indicated, a further complicating factor is where the digital information has been collected unlawfully in the state where the crime was committed: does this influence its admissibility as evidence?

As will become evident from the cases discussed below, some individuals and groups that may have committed international crimes have themselves chosen to document and publish videos and photographs of their actions via social media and other channels for propaganda purposes. Police and prosecutors have later made good use of this material during trial to prove crimes. This raises the question of the reliability of such evidence.

1 Principles of Flexible Admissibility and Free Evaluation of Evidence in Swedish Law

Two related issues are whether evidence is admissible and how individual pieces of evidence should be evaluated. Previously Sweden had a regulated approach to how to evaluate evidence: a model for admissibility and evaluation of evidence where the law lays down what evidence is admitted in certain cases, and the weight of different types of evidence. The principle *testis unus testis*

[1] Klamberg, Mark, *Evidence in International Criminal Trials: Confronting Legal Gaps and the Reconstruction of Disputed Events*, *Leiden: Martinus Nijhoff Publishers*, 2013, pp. 175 and 373; Krapiva, Natalia, *The United Nations Mechanism on Syria: Will the Syrian Crimes Evidence be Admissible in European Courts?*, California Law Review 2019, vol. 107, no. 3, 1101-1118, pp. 1103-1104 and 1107; Ekfeldt, Jonas, *Om informationstekniskt bevis*, Stockholm: Stockholms universitet, Juridiska institutionen, 2016, p. 332.

nullus (one witness is no witness) is an example of where the law provides how the Court should evaluate and weigh evidence.[2] Nowadays, Swedish criminal procedure relies on the principles of flexible admissibility and free evaluation of evidence.[3] However, an important limitation on admissibility is that the Court, pursuant to chapter 35 section 7 of the Code of Judicial Procedure (*Rättegångsbalken*), may exclude evidence that is "without importance in the case", i.e. irrelevant. However, there is no prohibition of certain types of evidence.[4] Whether evidence is relevant may thus be determined prior to or during trial – not necessarily during the concluding deliberations.[5] The principle of free evaluation of evidence is grounded in chapter 35 section 1 of the Code of Judicial Procedure. This provides that "After evaluating everything that has occurred in accordance with the dictates of its conscience, the court shall determine what has been proved in the case." From this follows that information from open sources and social media may be used as evidence if deemed relevant to the indictment.

However, one still has to respect the best-evidence rule[6] and the principle of immediacy.[7] Evidence from open sources and social media is not always the best evidence, especially where there is uncertainty as to how the evidence has been handled and stored. Nevertheless, photographs and especially film/video may constitute important evidence that may capture courses of events, facilitate identification of specific persons and establish how they have acted; and their presence at certain geographic locations.[8]

Despite difficulties for Swedish police and prosecutors to investigate alleged facts in another country, the same facts may have been investigated in other countries by international investigators or considered to be facts of common knowledge. According to Swedish law a Court may base its judgment on facts of common knowledge with no additional related evidence, nor is there a need for any of the parties to invoke these facts at trial.[9] The Inquiry on Procedural Law and Large Trials, SOU 2019:38, includes a discussion on the use of facts of common knowledge in relation to international crimes. The conclusion is that the judge may handle such facts as part of his or her power to organize pre-trial proceedings, with the following reasoning:

> In certain criminal cases – including cases of war crimes, crimes against international law and crimes against humanity – the uncertainty as to whether something can be

---

2 Ekelöf, Per Olof, Edelstam, Henrik & Heuman, Lars, *Rättegång IV*, 7th edn, Stockholm: Norstedts Juridik, 2009, pp. 26-27; Klamberg, 2013, p. 117; Lainpelto, Katrin, *Stödbevisning i brottmål*, Stockholm: Jure Förlag AB, 2012, p. 30.

3 Ekelöf, Edelstam & Heuman, 2009, p. 26.

4 Ibid, p. 34.

5 Klamberg, Mark, *Recension av Ulf Lundqvist, Laga och rättvis rättegång – Om bevisförbud i rättspraxis*, Juridisk Tidskrift 2015-16, nr. 4, 986-991, p. 987.

6 Chapter 35 section 12 Code of Judicial Procedure (Rättegångsbalken).

7 Chapter 30 section 2 Code of Judicial Procedure.

8 Ekfeldt, 2016, p. 329.

9 NJA II 1943 s. 203; chapter 35 section 2(1) Code of Judicial Procedure; Ekelöf, Edelstam, & Heuman, 2009, pp. 58-60.

> regarded as a fact of common knowledge causes significant difficulties during the proceedings. … For those cases where the fact at issue is a fundamental condition for establishing criminal responsibility, the evidence relied upon will be very extensive. An example is when the fact at issue is whether a genocide occurred at a certain place at a certain time, and the prosecution perceives this as common knowledge while the defendant disagrees, here the judge must sort out the parties' views on issues which may or may not be facts of common knowledge. We believe that the judge's power to organize the proceedings during the pre-trial proceedings includes raising the issue of facts of common knowledge with the parties. We find no grounds for suggesting formal rules on how judges should note facts of common knowledge, but this may be compared with the procedural framework for the Tribunal for Rwanda, where such rules do exist. (author's translation).[10]

2 Comparative Outlook on Admissibility and Evaluation of Evidence

Strict and technical provisions are primarily used in common-law systems. There are different possible explanations of why common-law countries have more formalized rules than continental (civil-law) European countries do. Civil-law systems combine the law- and the fact-finding functions by using professional judges. They have a flexible approach to admitting evidence. In common-law systems separation of the law and the fact-finding functions is more normal, allocating the former to the judge and the latter to the jury. One purpose of excluding certain evidence is to avoid the risk that the trier of fact – the jury – may rely on evidence that is perceived as unreliable, for example hearsay evidence. Formal rules on admissibility may also resolve the charge as promptly as possible, which implies that a party must not be allowed to waste time and increase cost by introducing irrelevant or prejudicial evidence.[11] The perception in civil-law systems is that there is less need to protect professional judges because they are not open to prejudice in the same way as a jury is. If the fact-finding is done with a combination of professional judges and lay judges (as in Sweden) the former may inform the latter of potential risks of certain evidence.[12] The rule skepticism in civil-law countries stems from bad experience of legal proof during the Middle Ages, when rigid rules requiring corroboration often led to confessions obtained by torture.[13]

---

10 Stora brottmål – nya processrättsliga verktyg, SOU 2019:38, p. 306.

11 Damaška, Mirjan R., *Evidentiary Barriers to Conviction and Two Models of Criminal Procedure: A Comparative Study*, University of Pennsylvania Law Review 1973, vol. 121, 506-589, p. 525; Zuckerman, A. A. S., *The Principles of Criminal Evidence*, Oxford: Clarendon, 1989, pp. 7 and 48-49; Boas, Gideon, "Admissibility of Evidence under the Rules of Procedure and Evidence of the ICTY: Development of the 'Flexibility Principle'" in May, Richard, Tolbert, David, Hocking, John, Roberts, Ken, Jia, Bing Bing, Mundis, Daryl & Oosthuizen, Gabriël (eds.), *Essays on ICTY Procedure and Evidence: In Honour of Gabrielle Kirk McDonald*, 263-274, The Hague: Kluwer Law International, 2001, p. 269; May, Richard & Wierda, Marieke, *International Criminal Evidence*, New York: Transnational Publishers, 2002, pp. 18 and 93; Klamberg, 2013, p. 335.

12 Klamberg, 2015-16, pp. 986-987; Krapiva, 2019, pp. 1111-1113.

13 Damaška, 1972-1973, p. 515; May and Wierda, 2002, p. 18; Klamberg, 2013, p. 336.

The absence of a jury has the consequence that international criminal courts such as the *ad hoc* tribunals for former Yugoslavia (ICTY), Rwanda (ICTR) and the International Criminal Court (ICC) have felt unhindered by technical rules for the admissibility of evidence. Instead they have emphasised weighing the totality of the evidence in accordance with the civil-law principle of "free evaluation of evidence".[14]

Freeman describes three periods which coincide with the time when international criminal courts were established and new types of evidence were used in the prosecution of international crimes. After the Second World War the Nuremberg prosecutors made use of the fact that Nazi Germany had documented huge amounts of information in registers, together with films and photographs. The registers were used to prove crimes while witness testimonies were given a less important role. In the ICTY and the ICTR trials of the 1990s new technologies were available. These included the use of DNA analysis, computers which could process large datasets, satellite imagery and the surveillance of communications, in addition to traditional evidence in the form of witness testimony and expertise in sociology, psychology and history. The establishment of the ICC coincided with a third technological wave where social media, interactive web services, smartphones and other mobile devices with cameras and global positioning systems; and drone technology. These technologies are not under the exclusive control of governments and their armed forces, but are available to large and expanding parts of the public. Thus information that would previously have disappeared is now being recorded and stored for possible use as evidence.[15]

International criminal tribunals and courts have relied upon audio and film recordings and photographs to corroborate witness testimony.[16] For example, the ICTR relied upon video footage and witness testimony to find that Colonel Bagosora was acting as Rwandan Minister of Defence and thus exercised control over the country's Armed Forces.[17]

The approach to the admissibility of illegally obtained evidence does not follow the traditional dividing line between common-law and civil-law systems. It appears that a balancing exercise is done in the French, English, German and U.S. systems, albeit with different considerations.[18] The exercise in France,

---

[14] *Prosecutor v. Blaškić*, (Case No. IT95-14-T), ICTY T. Ch., Judgment, 3 March 2000, para. 34; *Prosecutor v. Musema*, (Case No. ICTR-96-13-T), ICTR T. Ch., Judgment 27 January 2000, para. 75; *Prosecutor v. Thomas Lubanga Dyilo*, (Case No. ICC-01/04-01/06), ICC T. Ch. I, Decision on the admissibility of four documents, 13 June 2008, para. 24; May and Wierda, 2002, p. 93; Klamberg, 2013, p. 337.

[15] Freeman, Lindsey, *Digital Evidence and War Crimes Prosecutions: The Impact of Digital Technologies on International Criminal Investigations and Trials*, Fordham International Law Journal 2018, vol. 41, no. 2, 283-336, pp. 285-288 and 331-332.

[16] Dubery, Neha, *A New APP-reciation of Digital Evidence: Smartphones as Investigative Tools in International Criminal Law*: University of Leiden, 2016, p. 14.

[17] *Prosecutor v. Bagosora and Ors*, (Case No. ICTR-98-41-T), ICTR T. Ch. I, Judgment and Sentence 18 December 2008, paras. 2029-2031; *Prosecutor v. Bagosora and Nsengiyumva*, (Case No. ICTR-98-41-A), ICTR A. Ch., Judgment and Sentence 14 December 2011, para. 225

[18] Zuckerman, 1989, pp. 352-354; Delmas-Marty, M. & Spencer, J.R., *European Criminal Procedures*, Cambridge: Cambridge University Press, 2002, p. 605.

Germany and England tends to focus on the interests of the individual defendant, while societal interests such as sanctioning police misbehavior are emphasized in the US.[19] The European Court of Human Rights (ECtHR) stated in *Schenk v. Switzerland* that "[w]hile Article 6 (art. 6) of the Convention guarantees the right to a fair trial, it does not lay down any rules on the admissibility of evidence as such, which is therefore primarily a matter for regulation under national law". The Court decided that it "cannot exclude as a matter of principle and in the abstract that unlawfully obtained evidence [. . .] may be admissible".[20] However, the Court attached weight to the fact that the defence was allowed to challenge the authenticity of the recording and that the recorded telephone conversation was not the only evidence on which the conviction was based.[21] Rule 95 of each set of the rules of procedure and evidence of the ICTY and ICTR, and article 69(7) of the Rome Statute for the ICC, express a similar approach by balancing different interests where a distinction is made between minor infractions and more serious violations of the rights of the defendant. An example of the latter would be statements obtained by torture.[22]

2.1 Use of Digital Evidence, Smartphone Recordings and Social Media by International Courts and Domestic Courts

During the armed conflict in former Yugoslavia, communication was intercepted by military units other than those of the territorial state where the communication took place. This raised the issue of whether the intercepted communication could be used as evidence even though the national state authorities had not given prior approval for wire-tapping or surveillance. In other words, could illegally obtained digital information be admissible as evidence in court? In the *Kordić and Čerkez* case Judge May stated the following:

> [E]ven if illegality was established, . . . , we have to decide whether this is evidence obtained by methods which—the admission of which would be antithetical to and would seriously damage the integrity of the proceedings. We have come to the conclusion that . . . evidence obtained by eavesdropping on an enemy's telephone calls during the course of a war is certainly not within the conduct which is referred to in Rule 95. It's not antithetical to and certainly would not seriously damage the integrity of the proceedings.[23]

This meant that the evidence was admissible and could be used by the Prosecution. Similarly, in *Brđanin* the prosecution at the ICTY submitted for

---

19 Klamberg, 2013, pp. 398-399.

20 *Schenk v. Switzerland*, (Application No. 10862/84), ECtHR, Judgment, 12 July 1988, paras. 41 and 46. See also *Khan v. the United Kingdom*, (Application No. 35394/97), ECtHR, Judgment, 12 May 2000, para. 34; Björksved, Emilia, *Bevisvärdering av sociala medier - Facebook* (2013) Örebro universitet; Krapiva, 2019, pp. 1114-1116.

21 *Schenk v. Switzerland*, ECtHR, 12 July 1988, paras. 47 and 48.

22 Klamberg, 2013, pp. 400-406.

23 *Prosecutor v. Kordić and Čerkez*, (Case No. IT 95-14/2), ICTY T. Ch., oral decision delivered on 2 February 2000, 13694; see also quote in *Brđanin*, ICTY T. Ch., 3 October 2003, para. 19, footnote 23.

admission several transcripts of intercepted telephone conversations, recorded by internal security personnel of the government of the Republic of Bosnia and Herzegovina ("BiH") before and during the war. The defendant objected to the admission as evidence of all intercepted conversations on the ground that they were not authorized in accordance with the Constitution of the Republic and were thus illegally obtained. The *Brđanin* Trial Chamber considered that "admitting illegally obtained intercepts into evidence does not, in and of itself, necessarily amount to seriously damaging the integrity of the proceedings."[24] It also relied on the precedent established in *Delalić* et al., and recalled that "it would constitute a dangerous obstacle to the administration of justice if evidence which is relevant and of probative value could not be admitted merely because of a minor breach of procedural rules which the Trial Chamber is not bound to apply."[25] The *Brđanin* Trial Chamber stated that the "function of this Tribunal is not to deter and punish illegal conduct by domestic law enforcement authorities by excluding illegally obtained evidence."[26] It determined that the evidence at issue was relevant to the case, and admitted the evidence.[27] In *Naletilić & Martinović* the Appeals Chamber stated that the accused

> "must not only show that the Prosecution was under the obligation to seek the cooperation of the local authorities, but also that the failure to do so 'casts substantial doubt' on the reliability of the evidence in question or that its admission 'is antithetical to, and would seriously damage, the integrity of the proceedings'."[28]

The Prosecution's case against *Ayyash et al.* at the Special Tribunal for Lebanon (STL) relies heavily upon telecommunications data and records, including call data records – in other words metadata, information on who has called who.[29] The data had been lawfully registered and stored by national telecom operators. The key question was whether the data could be transferred to an international institution such as the STL, which would prevent oversight from national authorities and courts. This was not considered to be an obstacle since the STL was created by the UN Security Council. If judicial oversight were required, it should, as a matter of principle, come from either the UN or the Special Tribunal under their own rules and internal mechanisms, as opposed to

---

[24] *Brđanin*, ICTY T. Ch., 3 October 2003, paragraph 61; see also Krajišnik, ICTY T. Ch., 27 September 2006, para. 1189.

[25] *Brđanin*, ICTY T. Ch., 3 October 2003, paragraph 63–67 and *Prosecutor v. Zejnil Delalić et al.* (Čelebići), (Case No. IT-96-21), ICTY T. Ch., Decision on the Tendering of Prosecution Exhibits 104–108, 9 February 1998, para. 20.

[26] *Brđanin*, ICTY T. Ch., 3 October 2003, para. 63(9).

[27] *Ibid.*, paragraph 68.

[28] *Naletilić & Martinović*, ICTY A. Ch., 3 May 2006, para. 238.

[29] *Prosecution v Ayyash et al.*, Case No. STL-11-01/T/TC. Decision on Five Prosecution Motions on Call Sequence Tables and Eight Witness Statements and on the Legality of the Transfer of Call Data Records to UNIIIC and STL's Prosecution, 6 May 2015, paras. 1, 2, 4, 47-49.

those of national judges.[30] This is well in accordance with the principles discussed above.[31]

In cases at the ICC concerning Kenya, Côte d'Ivoire and Libya, video recordings taken with mobile devices, including smartphones, were used as evidence. Investigators found leads via Facebook and YouTube.[32] At the ICC the Prosecution has set up a special unit for the purpose, the Digital Forensics Team[33] within the Forensic Science Section (FSS). In the *Al Mahdi* case – which concerned the destruction of historic and religious buildings in Mali – satellite imagery, audio recordings found on the internet and videos from YouTube were used. The audio recordings, photographs and videos were used by rebel- and terrorist groups for recruitment and propaganda purposes. The defendant did not dispute the authenticity of the videos and agreed to their admission as part of a guilty plea.[34] In *Bemba* the prosecution relied upon photographs downloaded from the Facebook pages of two persons supporting the charge that the defendant had sought to influence the testimony of witnesses.[35] There are additional ICC cases with evidence from social media, including *Al-Werfalli* where the prosecution relied on videos published via Facebook.[36] In the Netherlands nine persons were convicted of terrorism for having incited, recruited, facilitated and financed youngsters who wanted to travel to Syria to fight there. The defendants had posted messages and/or images on social media such as Facebook and Twitter. From the judgment it appears that the focus was on the connection between the content of said material and the defendant without any substantial inquiry into whether the material was authentic and reliable.[37] It seems as if the Court has assumed that the evidence is admissible without questioning its authenticity or credibility.[38]

---

30 *Ayyash et al.*, STL T. Ch., 6 May 2015, paras. 90-107.

31 See section 2 "Comparative Outlook at Admissibility and Evaluation of Evidence".

32 Freeman, 2018, p. 289.

33 Mehandru, Nikita & Koenig, Alexa, *Open Source Evidence and the International Criminal Court*, Harvard Human Rights Journal (online) 2019.

34 *Prosecutor v. Ahmad Al Faqi Al Mahdi*, (Case No. ICC-01/12-01/15), ICC T. Ch. VIII, Judgment, 27 September 2016, para. 5; *Prosecutor v. Ahmad Al Faqi Al Mahdi*, (Case No. ICC-01/12-01/15), ICC T. Ch. VIII, Transcripts, 22 August 2016, pp. 28-29 and 36. See background and comment by Freeman, 2018, pp. 315-319.

35 *Prosecutor v. Jean-Pierre Bemba Gombo et al*, (Case No. ICC-01/05-01/13), ICC T. Ch. VII, Decision on Prosecution Requests for Admission of Documentary Evidence, 24 September 2015, see paras. 9 and 16 where the court waits with assessing the probative value of the picture until judgment; the pictures are not mentioned on the judgment, *Prosecutor v. Jean-Pierre Bemba Gombo et al*, (Case No. ICC-01/05-01/13), ICC T. Ch. VII, Judgment pursuant to Article 74 of the Statute, 19 October 2016.

36 *Prosecutor v. Mahmoud Mustafa Busayf Al-Werfalli*, (Case No. ICC-01/11-01/17), ICC PT. Ch. I, Warrant of Arrest, 22 August 2017, para. 11.

37 Rechtbank Den Haag, 8 June 2016, ECLI:NL:RBDHA:2015:16102 <http://uitspraken.rechtspraak.nl/inziendocument?id=ECLI%3ANL%3ARBDHA%3A2015%3A16102> (non-official translation to English), see especially section 5.

38 Dubery, 2016, p. 33

2.2 Comparative Outlook on Judicial Notice of Facts of Common Knowledge and Adjudicated Facts

Considering procedural economy, i.e. the sound administration of a court's resources, there may be reasons to deviate from the principle of immediacy in relation to circumstances that are commonly or universally known, i.e. facts of common knowledge. The possibility of basing a judgment on common knowledge existed and exists in the ICTY, the ICTR, the Special Court for Sierra Leone (SCSL), the Extraordinary Chambers in the Courts of Cambodia (ECCC) and the ICC.[39] Judicial notice also allows the fact-finder to accept adjudicated facts. Article 21 of the International Military Tribunal (Nuremberg) Charter provided that the Tribunal could take judicial notice of the "records and findings of military or other Tribunals of any of the United Nations."[40] Similarly, pursuant to ICTY, ICTR, SCSL rule 94(B) and to International Residual Mechanism for Criminal Tribunals rule 115(B), the Chamber may at the request of a party or *proprio motu* take judicial notice of adjudicated facts. The ICC has no equivalent to rule 94(B) of the ad hoc tribunals, which would allow a Chamber to admit adjudicated facts under the power of judicial notice.[41]

In the *Simić et al.* case the prosecution requested the ICTY Trial Chamber to take judicial notice of the international character of the conflict either as a fact of common knowledge or an adjudicated fact based on the findings in *Tadić* and *Delalić et al.*[42] The characterisation of a conflict is important since it determines the applicable legal framework and which acts are criminalized, as illustrated in the *Arklöv* case.[43] The Trial Chamber in *Simić et al.* ruled that findings as to the international character of the conflict had no binding force except between the parties in respect of a particular case. Nevertheless the Chamber considered that Bosnia and Herzegovina's proclamation of independence on 6 March 1992, and its recognition by the European Community on 6 April 1992 and by the United States on 7 April 1992, were facts of common knowledge under Sub-Rule 94(A),

---

39 IMT Charter, article 21; IMTFE Charter, article 13(d); ICTY, ICTR, SCSL RPE regel 94(A) and IRMICT RPE rule 115(A)

40 The name United Nations originally referred to the nine occupied European countries who signed the St. James Declaration in January 1942 which later grew to the thirty-two States mentioned in the Moscow Declaration 30 October 1943, see also Sprecher, Drexel A., *Inside the Nuremberg Trial: a Prosecutor's Comprehensive Account*, vols I and II, Lanham/New York/Oxford: University Press of America, 1999, p. 22 and United Nations Declaration, 1 January 1942 reprinted in Russell, R.B., & Muther, J.E., A History of the United Nations Charter: The Role of the United States 1940–1945, 1958, 976.

41 However, see the cautious decision in *Prosecutor v. Jean-Pierre Bemba Gombo et al*, (Case No. ICC-01/05-01/13), ICC T. Ch. VII, Decision on Prosecution Request for Judicial Notice, 9 November 2015.

42 *Prosecutor v. Dusko Tadić*, (Case No. IT-94-1), ICTY T. Ch., Opinion and Judgment, 7 May 1997; *Prosecutor v. Zejnil Delalić et al. (Čelebići)*, (Case No. IT-96-21), ICTY T. Ch., Judgment, 16 November 1998.

43 *Prosecutor v. Jackie Arklöv*, Stockholm district court, Case no. B 4084-04, Judgment of 18 December 2006, pp. 52-55.

of which the Trial Chamber *proprio motu* took judicial notice.[44] ICTR Rule 94(A) and ICTY Rule 94(A) are mandatory: if a Trial Chamber determines that a fact is "of common knowledge", it must take judicial notice of it.[45] Article 69(6) of the Rome Statute is phrased in a less strict manner as it uses the word "may" instead of "shall".

3 Review of Swedish Case Law

The next sections describe how digital evidence, facts of common knowledge and adjudicated facts have been dealt with by Swedish courts. There are other, distinct evidentiary issues for this kind of case, for example allegations that Rwandan state officials had sought to influence witnesses.[46] Comb's study of the ICTR may be of interest in this context.[47] However, it is only possible to give an account of a select number of issues.

3.1 Digital Evidence, Smartphones, Open Sources and Social Media in Swedish Courts

The Swedish National Forensic Centre (NFC: *Nationellt forensiskt centrum*) conducts forensic investigations and analyses on behalf of the judicial authorities. The NFC uses a unified scale of conclusions based on likelihood ratios that are applied to all casework that involves evaluative statements. The scale has nine levels from "-4 The results extremely strongly support that.. [alternative hypothesis] … " to "+4 The results extremely strongly support that.. [main hypothesis]".[48]

In the *Droubi* case the police had obtained a video recording of the violence at hand which led to the detention of the defendant. The video recording shows how Droubi and other persons belonging to the same group are assaulting another person and issuing death threats. Initially during the investigations Droubi denied that he was the person in the video recording; however at trial he admitted that he had assaulted the victim but denied criminal responsibility, *inter alia*, because of duress. Droubi explained that he had found the film on a Syrian

---

[44] *Prosecutor v. Simić*, (Case No. IT-95-9), ICTY T. Ch., Decision on the Pre-Trial Motion by the Prosecution Requesting the Trial Chamber to Take Judicial Notice of the International Character of the Conflict in Bosnia-Herzegovina, 25 March 1999.

[45] *Prosecutor v. Karemara et al.*, (Case No. ICTR-98-44-AR73(C)), ICTR A. Ch., Decision on Prosecutor's Interlocutory Appeal of Decision on Judicial Notice, 16 June 2006, para. 22. Comment by Klamberg, 2013, pp. 472-473.

[46] *Prosecutor v. Tabaro*, Stockholm district court, judgment, 27 June 2018, pp. 146-171; *Prosecutor v. Tabaro*, Svea Hovrätt, Mål B 6814-18, judgment, 29 April 2019, pp. 21-23.

[47] Combs, Nancy Amoury, *Fact-Finding Without Facts - The Uncertain Evidentiary Foundations of International Criminal Convictions*, New York: Cambridge University Press, 2010; Combs, Nancy Amoury, *Grave Crimes and Weak Evidence: A Fact-Finding Evolution in International Criminal Law*, Harvard International Law Journal 2017, vol. 58, no. 1, 47-125.

[48] Swedish National Forensic Centre, Scale of Conclusions, 9 January 2019, available at https://nfc.polisen.se/siteassets/dokument/ovrigt/scale-of-conclusions.pdf.

news site and had posted it on Facebook on at least three occasions because he wanted to prove that he was not loyal to the regime, or a spy.[49] At the request of the police the NFC evaluated the authenticity to see whether the recording was manipulated, for example that it had been dubbed by another voice. There was an attempt to establish on what medium the film had been recorded. The conclusions of the forensic investigation regarding speech and image were that that the results strongly supported (grade 3+) that the film had not been manipulated. No reliable conclusion could be drawn about the date of the recording.[50]

While the use of evidence in social media in the *Droubi* case was fairly uncomplicated since he admitted he was in the recording, the challenge was greater in the *Al-Mandlawi and Sultan* case. This concerned the execution of two men which was recorded in three videos. One of the difficulties was that the perpetrators had their faces covered with scarves. Instead, identification was based on tattoos visible in the videos, and on voice analysis. The NFC found that the results of their analysis determined with *extreme certainty* that Sultan was in the first video, and that the analysis *extremely strongly* supported that Al-Mandlawi was in all three videos with a Palestinian *keffiyeh* (black and white scarf) on his head. Moreover, the results of the voice analysis strongly supported that Al-Mandlawi was one the persons speaking in the video.[51] The NFC conducted the analysis by pitting the investigation's main hypothesis against an alternative hypothesis.[52] There were also statements which indicated that the expert had used automated biometric voice analysis which, *inter alia*, can be used to determine the likelihood ratio that the speech came from same voice compared with the probability of its coming from a different voice in a given population. [53] The district court found it proven by the videos that the two men had been executed. Given the NFC report, the district court found no reason to question the authenticity of the videos. The court noted physical attributes in relation, *inter alia*, to ear, nose, body size, hair, beard, scars and tattoos and that the person in the video spoke Swedish – which reduces the risk of mix-up in identification. Based on the videos, the NFC analysis and that one of the videos showing the execution was found on a USB flash drive in the possession of one of the defendants, the district court found it proven that the defendants were identical to the perpetrators shown in the execution videos.[54] On appeal, the Court of Appeal for Western Sweden reached the same conclusion.[55]

---

[49] *Prosecutor v. Droubi*, Svea Hovrätt, Mål B 4770-16, judgment, 5 August 2016, pp. 6 and 20.

[50] *Prosecutor v. Droubi*, Södertörn district court, Mål B 2639-16, aktbilaga 8, förundersökningsprotokoll, 3 March 2016, pp. 73-76 (expert opinion from SKL, diarie nr: 0104-K513-14, 21 November 2014) and pp. 33, 49, 95, 105-140 (excerpt from Facebook account and protocol 8 January 2015).

[51] *Prosecutor v. Al-Mandlawi and Sultan*, judgment, 14 December 2015, pp. 7-8.

[52] *Prosecutor v. Al-Mandlawi and Sultan*, Göteborg district court, Mål B 9086-15, aktbilaga 127, förundersökningsprotokoll (redacted) 23 November 2015, p. 64.

[53] Ibid, p. 87.

[54] *Prosecutor v. Al-Mandlawi and Sultan*, judgment, 14 December 2015, pp. 20-26.

[55] *Prosecutor v. Al-Mandlawi and Sultan*, Hovrätten för Västra Sverige, judgment, 30 March 2016, p. 4.

The evidentiary issues in *Abdulkareem* are similar to those in the *Droubi* case in that Abdulkareem had published two images on Facebook. They showed how Abdulkareem dressed in combat gear is standing next to two desecrated bodies. Abdulkareem admitted that it was him in the images, thus the district court found the indictment proven based on the images, the material on Facebook and the confession in relation to the alleged facts.[56] In the *Haisam Sakhanh* case the defendant belonged to a rebel group and posed next to captured government soldiers – i.e. from the opposing side in the conflict – all documented in a video. Shortly afterwards the prisoners were executed. The execution and subsequent events were recorded and documented in the video. The prosecutor's investigation material (*förundersökningsprotokoll*) states that the video had been obtained by the police from Amnesty without information on who gave it to Amnesty.[57] Other videos had been published by the rebel group on YouTube,[58] including an audio recording of the execution.[59] The NFC had compared the image of the perpetrator in the execution movie with one of the defendant, and this led to *strong* support for the conclusion that it was the same person. There was extremely strong support for the finding that the video had not been manipulated. The conclusion was that Haisam Sakhanh had fired at least six shots. The district court found the probative value of the video to be very strong.[60] The defendant confessed that he had participated in the execution in the manner alleged by the prosecutor, but denied criminal responsibility since he had implemented death sentences issued by a legitimate court.[61] In the *Saeed* case the police found images published on the defendant's Facebook pages. Forensic investigation found logins on Facebook in Iraq as well as later when he had arrived in Sweden. Photos were subsequently found on a USB flash drive and in a computer.[62] Saeed had handed in the USB flash drive to the Migration Agency when applying for asylum in Sweden.[63] The NFC conducted a forensic investigation and found no signs that the photos had been manipulated. [64] The *Abdullah* case also concerned a photo showing how the defendant posed and was photographed in front of wounded and killed persons from the opposing side of the conflict. The difference was that the photo was not found on social media or

---

[56] *Abdulkareem,* Blekinge district court, Mål B 569-16, judgment, 6 December 2016, pp. 3-4, 10-13, 16. Se även *Abdulkareem,* Hovrätten över Skåne and Blekinge, judgment, 11 April 2017, p. 2.

[57] *Prosecutor v. Omar Haisam Sakhanh*, Stockholm district court, B 3787-16, förundersökningsprotokoll, aktbilaga 82, 28 December 2016, pp. 928 and 945. Compare with NJA 1998 s. 204.

[58] *Sakhanh*, Stockholm district court, judgment 16 February 2017, pp. 6 and 20.

[59] *Sakhanh*, Stockholm district court, förundersökningsprotokoll, aktbilaga 82, 28 December 2016, p. 931, film 8.

[60] *Sakhanh*, Stockholm district court, judgment 16 February 2017, p. 21; see *Sakhanh*, Stockholm district court, förundersökningsprotokoll, aktbilaga 82, 28 December 2016, pp. 1002, 1005, 1012-1013 and 1017 för NFCs utlåtande.

[61] *Sakhanh*, Stockholm district court, judgment 16 February 2017, p. 9.

[62] *Saeed*, Örebro district court, judgment 19 February 2019, pp. 13-14.

[63] Ibid, p. 14.

[64] Ibid, p. 10.

on digital medium. Here the police, following a tip, had had the photo sent to them.[65] In the indictment the Prosecutor referred to an NFC expert opinion that the photo had not been manipulated.[66] However, the district court did not mention the expert opinion or state how it viewed the authenticity of the photo. This is probably explained by the defendant's admission that it was him in the photo.[67] However, Droubi, Abdulkareem and Haisam Sakhanh also admitted this in their cases. In these cases the district court still made assessments on authenticity and reliability.[68] From these few cases it appears that the courts perceive a need to test the authenticity of photos and videos in digital form.

3.2 The Use of Facts of Common Knowledge and Adjudicated Facts before Swedish Courts

As mentioned above, Swedish law provides that a court may base its judgment on facts of common knowledge with no additional evidence relating to these facts: there is not even a need for a party to invoke these facts at trial.[69] To adjudicate facts is not a mechanism mentioned in the Swedish Code of Judicial Procedure.[70] In *Mbanenande*, *Berinkindi* and *Tabaro* there are references to ICTR assessments of factual circumstances in Rwanda.[71] The same phenomena may be observed in the *M.M.* case, where the district court refers to ICTY cases in order to assess the factual circumstances in Kosovo.[72] Thus, the district courts in the cases mentioned appear to base their judgments on facts – or evidence – adjudicated by international courts. Reliance on adjudicated facts is a mechanism explicitly provided for in the Rules of Procedure and Evidence (RPEs) of the ICTY and ICTR but not in the Swedish Code of Judicial Procedure.[73] It is relevant that the defendants did not deny adjudicated facts such as whether there was a non-international armed conflict in Rwanda, or that widespread killing and

---

65 *Prosecutor v. Abdullah*, judgment, 25 September 2017, p. 3.

66 Page 2 of the indictment, attached to the judgment.

67 *Prosecutor v. Abdullah*, judgment, 25 September 2017, p. 13.

68 Compare with Ekfeldt, 2016, p. 330.

69 NJA II 1943 s. 203; Chapter 35 section 2(1) Code of Judicial Procedure; Ekelöf, Edelstam, & Heuman, 2009, pp. 58-60.

70 SOU 2017:7, bilaga 6, pp. 193-194.

71 *Mbanenande*, Stockholm district court, 20 June 2013, p. 36, para. 6 which refers to *Akayesu*, ICTR T. Ch., 2 September 1998, paras. 619-621 and 627 where the material shows that it was a non-international armed conflict; *Berinkindi*, Stockholm district court, judgment 16 May 2016, pp. 136-137 refers to *Akayesu*, ICTR T. Ch., 2 September 1998: "The investigation and the case law from the ICTR shows that at the time there was a non-international armed conflict between the Government armed forces FAR on one side and the invasion troops RPF on the other side"; *Tabaro*, 27 June 2018, p. 141 to *Ntagerura m.fl.*., ICTR-99-46-T, pp. 175-176 to *Akayesu*, ICTR T. Ch., 2 September 1998 that the genocide in Rwanda aimed to destroy the Tutsi group.

72 *M.M.*, Stockholm district court, judgment 20 January 2012, pp. 47-48 *Limaj et al.*, ICTY T. Ch. II, 30 November 2005, paras. 171-173; *Đorđević*, ICTY T. Ch., 23 February 2011, para. 1579; *Milutinović et al.*, ICTY T. Ch., 26 February 2009, para. 1217.

73 ICTY RPE, rule 94(B); ICTR RPE, rule 94(B); Klamberg, 2013, pp. 474-476.

genocide occurred. Instead the defendants refuted their participation, the identification and attribution of guilt made in relation to them.[74] Turning to the use of facts of common knowledge, the district court in Saeed stated that "it is a fact of common knowledge that IS … is an armed group".[75]

4 Analysis

It appears as Swedish courts seek to apply the same rules and principles of admitting and evaluating evidence in cases relating to international crimes as the Swedish courts would usually apply in "normal" cases. However, trials involving international crimes may raise special challenges that warrant a discussion, not least when it comes to digital evidence, judicial notice of facts of common knowledge and adjudicated facts.

The use of digital evidence raises important questions regarding fair trial rights, equality of arms, and a balance in resources between the prosecution and the defence. As indicated earlier issues relating to how evidence has been collected and handled (chain of custody) may become paramount for determining a case. Amann and Dillon argue that the following needs to be documented:[76]

- Where, when and by whom was the evidence discovered and collected?
- Where, when and by whom was the evidence handled or examined?
- Who had custody of the evidence and during what period?
- How was it stored?
- When the evidence changed custody, when and how did the transfer occur?

One challenge with digital evidence is that it is volatile and manipulable. Law enforcement agencies can take protective measures and implement procedures to guarantee that the material has been in handled in a correct manner. Amann and Dillon suggest that this can be done by running an algorithm over the binary content of the file and creating a unique "hash value". This unique value may be registered on the chain-of-custody form. If later there is any doubt about the authenticity of the file, the same algorithm can be run again. It will remain the same if the content has not been altered. Digital forensics offers additional tools and procedure to collect and examine evidence that has been stored on digital media. This requires a proactive approach, training, standardization of practice, and the right hardware and software.[77]

---

74 *Mbanenande*, Stockholm district court, 20 June 2013, p. 26; *Mbanenande*, Svea Hovrätt, 19 June 2014, p. 5; *Berinkindi*, Stockholm district court, judgment 16 May 2016, p. 31; *Prosecutor v. Tabaro*, Stockholm district court, judgment, 27 June 2018, p. 33.

75 *Saeed*, Örebro district court, judgment 19 February 2019, p. 9.

76 Amann, Philipp & Dillon, Mark P., "Electronic Evidence Management at the ICC: Legal, Technical, Investigative and Organizational Considerations" in Babington-Ashaye, Adejoké, Comrie, Aimée & Adeniran, Akingbolahan (eds), *International Criminal Investigations: Law and Practice*, 231-252, The Hague: Eleven International Publishing, 2018, p. 237.

77 Amann, Philipp & Dillon, Mark P., "Electronic Evidence Management at the ICC: Legal, Technical, Investigative and Organizational Considerations" in Babington-Ashaye, Adejoké, Comrie, Aimée & Adeniran, Akingbolahan (eds), *International Criminal Investigations: Law*

In several of the Swedish cases which have relied upon digital evidence, the defendants have admitted the factual circumstances alleged by the prosecutor; but the courts were still discussing – with the exception of the district court in the *Abdullah* case – the authenticity and reliability of photo and video. This is a reasonable approach taken by the courts since confessions and admissions of factual circumstances are not binding upon the court in criminal cases. Such confessions and admissions are to be assessed[78] and more evidence is needed before firm conclusions are drawn. These are procedural safeguards which reflect the truth-seeking aspect in the administration of justice. The use of digital evidence requires resources which may put the defence at a disadvantage vis-à-vis the police and prosecution. To compensate, it is necessary that either the defence receive more resources during the investigations, that the defence may request that the police investigations are conducted in the interest of the defendant or that the police thus on its own initiative investigates pursuant to the principle of objectivity.

It was especially necessary in the *Al-Mandlawi and Sultan* case for the district court to consider the reliability and probative value of the digital evidence submitted in view of the defendants' denial that it was them in the videos. This does not mean that the digital evidence submitted in the other cases was unnecessary; in several cases it was the videos that triggered the start of investigations, and the videos showed criminal acts which made it difficult for the suspects (later defendants) to refute.

There is a tendency to portray digital evidence as something essentially different from other evidence. Digital evidence may particularly be challenged and called into question when it has changed custody or storage medium several times, since this may make it more difficult for police and prosecution to prove that the material has been correctly handled without being manipulated. Forensic investigations may partly compensate and confirm the authenticity of the evidence. However, this and similar problems are also present in relation to printed documents and photographs where there are several stages and/or persons between the criminal act and the evidence reaching police custody. Yet there *is* a fundamental difference since digital evidence requires access to hardware and software. With ongoing technological evolution some digital information is no longer available on all operative systems.[79] Digital evidence may also be more reliable in certain regards than testimonial evidence – it may be recorded directly as an event occurs. Several social networking services have functions which reveal the date and time when postings have been made, in some cases from where the post was made through so called checks-ins. That means that state agencies – including the police and prosecution - and courts with a high degree of reliability may determine where a person was or what that person did at a given point of time.[80]

---

and Practice, 231-252, The Hague: Eleven International Publishing, 2018, pp. 237-243 and 252.

78 Chapter 35 section 3(2) Code of Judicial Procedure.

79 Mehandru and Koenig, 2019.

80 Björksved, 2013, p. 16. *Prosecutor v. J.O.*, Hovrätten för nedre Norrland, Mål B 231-13, judgment 19 April 2013, p. 7.

There are also reasons to expect that the use of and reliance on digital evidence will increase. It is probable that increased access to drones with high-resolution cameras will lead to an increased prevalence of video evidence. Organisations present within and outside of Syria have collected films from social media and other documentation from the internet that can be used as evidence in domestic criminal trials. The increasing amount of available information may be a curse as well as a blessing: it may overload investigators.[81]

The courts do not appear to have reflected in depth on the use of facts of common knowledge and adjudicated facts. A certain degree of pragmatism may be warranted at the same time as the interests of all parties are being considered, especially those of the defence. If a fact at issue is not contended, has been scrutinized in a previous case or is perceived as being a fact of common knowledge and does not concern the defendant's personal actions or connection to the alleged act, the court should, for reasons of procedural economy, be able to find the fact as proven. However, if a fact at issue is disputed and contended by the defence, but has relevance when assessing the guilt of the defence, other additional evidence must be submitted and assessed during the trial.

Literature

Amann, Philipp & Dillon, Mark P., "Electronic Evidence Management at the ICC: Legal, Technical, Investigative and Organizational Considerations" in Babington-Ashaye, Adejoké, Comrie, Aimée & Adeniran, Akingbolahan (eds.), *International Criminal Investigations: Law and Practice*, 231-252, The Hague: Eleven International Publishing, 2018

Björksved, Emilia, *Bevisvärdering av sociala medier – Facebook*, Örebro universitet, 2013

Boas, Gideon, "Admissibility of Evidence under the Rules of Procedure and Evidence of the ICTY: Development of the 'Flexibility Principle'" in May, Richard, Tolbert, David, Hocking, John, Roberts, Ken, Jia, Bing Bing, Mundis, Daryl & Oosthuizen, Gabriël (eds.), *Essays on ICTY Procedure and Evidence: In Honour of Gabrielle Kirk McDonald*, 263-274, The Hague: Kluwer Law International, 2001

Combs, Nancy Amoury, *Fact-Finding Without Facts - The Uncertain Evidentiary Foundations of International Criminal Convictions*, New York: Cambridge University Press, 2010

Combs, Nancy Amoury, *Grave Crimes and Weak Evidence: A Fact-Finding Evolution in International Criminal Law*, Harvard International Law Journal 2017, vol. 58, no. 1, 47-125

Damaška, Mirjan R., *Evidentiary Barriers to Conviction and Two Models of Criminal Procedure: A Comparative Study*, University of Pennsylvania Law Review 1973, vol. 121, 506-589

Delmas-Marty, M. & Spencer, J.R., *European Criminal Procedures*, Cambridge: Cambridge University Press, 2002

Dubery, Neha, *A New APP-reciation of Digital Evidence: Smartphones as Investigative Tools in International Criminal Law*, University of Leiden, 2016

[81] Freeman, 2018, p. 332.

Ekelöf, Per Olof, Edelstam, Henrik & Heuman, Lars, *Rättegång IV*, Stockholm: Norstedts Juridik, 7th ed, 2009

Ekfeldt, Jonas, *Om informationstekniskt bevis*: Stockholms universitet, 2016

Freeman, Lindsey, *Digital Evidence and War Crimes Prosecutions: The Impact of Digital Technologies on International Criminal Investigations and Trials*, Fordham International Law Journal 2018, vol. 41, no. 2, 283-336

Klamberg, Mark, *Evidence in International Criminal Trials: Confronting Legal Gaps and the Reconstruction of Disputed Events*, Leiden: Martinus Nijhoff Publishers, 2013

Klamberg, Mark, Recension av Ulf Lundqvist, Laga och rättvis rättegång – Om bevisförbud i rättspraxis, Juridisk Tidskrift 2015-16, no. 4, 986-991

Klamberg, Mark, "Bevisföring och bevisvärdering i internationell och digital kontext", in Klamberg, Mark (ed.), *Lagföring i Sverige av Internationella Brott*, Stockholm: Jure 2020, 355-368

Krapiva, Natalia, *The United Nations Mechanism on Syria: Will the Syrian Crimes Evidence be Admissible in European Courts?*, California Law Review 2019, vol. 107, no. 3, 1101-1118

Lainpelto, Katrin, *Stödbevisning i brottmål*, Stockholm: Jure Förlag AB, 2012

May, Richard & Wierda, Marieke, *International Criminal Evidence*, New York: Transnational Publishers, 2002

Mehandru, Nikita & Koenig, Alexa, *Open Source Evidence and the International Criminal Court*, Harvard Human Rights Journal (online) 2019

Sprecher, Drexel A., *Inside the Nuremberg Trial: a Prosecutor's Comprehensive Account*, vol I and II, Lanham/New York/Oxford: University Press of America, 1999

Zuckerman, A. A. S., *The Principles of Criminal Evidence*, Oxford: Clarendon, 1989