Digital Evidence and Criminal Defense

How International Standards Apply in German Criminal Proceedings

An initiative of the Center for International Human Rights (CIHR) at John Jay College of Criminal Justice, City University of New York (CUNY)

Digital Evidence and Criminal Defense: How International Standards Apply in German Criminal Proceedings

Author:

Carsten Momsen, Ph.D., *Visiting Scholar, Center for International Human Rights and Chair of Comparative Criminal Law, Criminal Procedure, Economic and Environmental Criminal Law, Freie Universität Berlin*

Contributing Editor:

Marie-Michelle Strah, Ph.D., *Visiting Scholar, Center for International Human Rights and Adjunct Professor of International Crime and Justice, John Jay College of Criminal Justice*

Date of Publication: September 2021

I. Introduction

At present, a large proportion of evidence in criminal trials is already produced in digital format; collected and preserved as digital data in connection with criminal proceedings. However, the presentation or utilization of the data in the main criminal trial regularly takes place in non-digital form. One example is the seizure of e-mails, which only become documentary evidence in printed form at a relatively late point in time, and may also become an object of inspection, or recordings of telephone conversations, a large proportion of which are already digitized using VoIP (Voice over IP). Digitization is therefore an (initially empirical-factual) phenomenon to which the German laws of evidence in criminal proceedings must react at very different procedural steps.[1] In this white paper, I will discuss various aspects of digital evidence and its implications for German criminal proceedings, with reference to both human rights law and examples from common law (specifically the United States).

For example, in 2007, Julie Amero, a substitute teacher at a school in Connecticut in the United States, was charged with showing pornographic content to her students on a school computer. She faced a maximum 40-year prison sentence.[2] During class, Amero had turned on the computer when pop-ups suddenly opened with pornographic content. According to her own account, when the children became aware of the images, which she herself had not noticed at first, Amero stood in front of the computer and ordered her students out of the room. However, she was unable to prevent several children from becoming aware of the images. An analysis of the log files in the preliminary investigation revealed that corresponding files had been called up. For formal procedural reasons, the trial court prohibited an expert investigation into the question of whether the call could have been caused by so-called "malware" that was loaded via the browser without authorization.

However, with the help of experts from the field of digital forensics, it was then possible to show on appeal that a "NewDotNet" spyware that had been installed on the computer a few days earlier had triggered pop-ups of pornographic content that could not be controlled by the respective user of the computer. This means Amero herself had presumably in no way called up the incriminated pages himself, and certainly not consciously.[3] The evidentiary value of the call logs themselves was close to zero with regard to the criminally relevant question of whether the defendant had committed a corresponding offense

---

[1] Unfortunately, the current and otherwise very informative “Alternative Draft on German Evidence Law” (AE-Beweisrecht, GA 2014,1 ff.) completely ignores these questions, as does the equally intense discussion about the use of evidence obtained in the course of private investigative measures. There are many overlaps and resulting legal questions between these two areas, which are becoming increasingly important in the practice of obtaining evidence (see below). Very instructive, however, is, for example, *National Research Council*, Strengthening Forensic Science in the United States: A Path Forward, 2009; *Casey* in: Casey (ed.), Digital Evidence and Computer Crime, 3rd Edition, 2011 - "Digital Evidence in the Court Room," pp. 49 ff. ; *Endicott-Popovsky/Horowitz*, Unintended Consequences: Digital Evidence in Our Legal System, Washington State Bar News, August 2012, pp. 11 ff.; *Marshall*, Digital Forensics - Digital Evidence in Criminal Investigation, 2008; *Ryan/Shpantzer*, Legal Aspects of Digital Forensics, available at: http://euro.ecom.cmu.edu/program/law/08-732/Evidence/RyanShpantzer.pdf; *Singelnstein*, NStZ 2012, 593 ff; *Tan*, Forensic Readiness, http://www.atstake.com/ research/ reports/ acrobat/ atstake_forensic_readiness.pdf.
On individual technical and procedural aspects: *Hercher/Momsen*, Digitale Beweismittel im Strafprozess - Eignung, Gewinnung, Verwertung, Revisibilität**,** in: Akzeptanz des Rechtsstaats in der Justiz, 2013, Materialband zum 36. Strafverteidigertag in Freiburg i.Br. vom 8.-10.März 2013, 2014; *Rudolph*, Akzeptanz des Rechtsstaats in der Justiz, 2013, Materialband zum 36. Strafverteidigertag in Freiburg i.Br. vom 8.-10.März 2013, 2014; *Geschonneck*, Computer-Forensik, 2004.

[2] More closely *Endicott-Popovsky/Horowitz* (fn.1), p. 11.

[3] The report of one of the expert witnesses who was initially denied admission on formal grounds is instructive: *Boyko*, Service Assurance Daily, January 22, 2007, "The Strange Case of Ms. Julie Amero: Commentary by Mr. *Herb Horner*."

responsibly. And this, although it was initially considered in the first instance as the decisive incriminating evidence, whose "objective" evidentiary value for the proof of the crime only required supplementation by witness statements (of the students).

II. Digital Evidence in Germany

Looking at the Amero case from a German perspective, one will have to concede that in procedural terms, i.e. with regard to the evaluation of evidence, there are no significant differences here, notwithstanding the "Rules of Evidence" specific to common law.[4] Furthermore, it does not even seem to be a problem that is exclusively inherent in the digital nature of the evidence, although specific knowledge in the area of so-called "digital forensics" was necessary in order to be able to recognize the potential defectiveness. [5] Nevertheless, the scope and quality of all evidence must always be checked. Fingerprints, handwriting samples and DNA identification samples also require specific expert knowledge. Nor does the fact that evidence is available in digital form (necessarily) change its procedural character. For this reason, the legal relevance of designating evidence as "digital" could at first glance be seen as of little significance from the perspective of a highly formalized regulatory system such as that of criminal proceedings with clearly defined forms of evidence.

Yet it is precisely the formalization due to which the digital nature of evidence can develop far-reaching consequences for the process of establishing the truth. Not only evidence suitability and value, but new forms of evidence manipulation have to be considered. Already the application of the traditional categorization of evidence requires the definition of (new) boundary lines. For the digital data must be made (sensorially) perceptible, transformed, as it were, into evidence in the first place.

A central principle of the taking of evidence in criminal proceedings is the principle of immediacy. This means, on the one hand, that the closest evidence is to be used. The probative value of the witness who has observed an incident himself is to be preferred to the testimony of the official who has heard the actual witnesses. On the other hand, the evidence must be presented directly in the main hearing. Thus, the witness must testify him or herself; the reading of a written or recorded statement is allowed only in exceptional cases. In this sense, digital data cannot be taken directly as evidence, since the content embodied in it is not immediately perceptible. Nor can digital information be compared with documentary evidence, since they do not represent - comparable to written language - ciphers that can be understood by everyone; this is evident pars pro toto in the case of a digitized telephone recording.

The testimony of an interrogator has less probative value than the actual subject matter of the evidence because, to a certain extent, an additional filter is interposed between the facts perceived and those reflected in the main hearing. In this respect, the collection of evidence is only indirect, as has been shown. Every filter, every mediation, however, creates the risk of information selection. However, selection is always interpretation and reduction at the same time. The conversion process required for transforming digital data into evidence that can be used in proceedings harbors a very comparable potential for interpretation and reduction. If the conversion to evidence is carried out by automated

[4] For their current status, see. Federal Evidence Review 2014, p. 1 ff.
[5] Good overview of the increasing importance of digital evidence against the background of developments in IT in *Marshall* (fn.1), p. 9 ff.

processes, the focus is on the reduction problem, the threat of loss of evidence. If the conversion is carried out by human interpretation processes, the risk of manipulation of the evidence content predominates.

On the one hand, this applies to the handling of digital data secured for evidentiary purposes by law enforcement authorities. On the other hand - and here we are largely in the dark or unaware of the risks for criminal proceedings - data secured for evidentiary purposes can easily become the target of hacking attacks. I will come back to this. From the perspective of the defense, it must therefore be asked whether the only indirect evidentiary suitability inherent in the nature of the evidence results in a fundamentally lower probative value. For this reason alone, the equally widespread and irrational assumption that digital evidence is endowed with a kind of specific "objectivity" is obviously incorrect. It is mostly interpretation and depends on various subjective prerequisites like the selection of incoming data and composition of samples, design of algorithms, education and awareness of flaws and biases just to point out some issues.[6]

1. Increasing Importance of Digital Information - Increasing Importance of Digital Evidence

Digital evidence is already used in the majority of all non-witness statement evidence.[7] Content and information are additionally, but increasingly also exclusively, created and disseminated digitally. Business is conducted online; EDP systems can be found in almost all companies. Text documents as well as photo, video and audio recordings are now predominantly created and stored digitally. Private communications are also largely carried out in digital form. At the same time, the volume of data and the number of devices involved in the exchange of information is increasing significantly. The "Internet of Things," i.e., the integration of many devices that are not primarily used for communication, such as cars or "smart" household appliances, leads to an immense number and variety of possible sources of information about the behavior of individual persons. This flood of information must be filtered using algorithm-based "big data" concepts and made effectively manageable. In addition, cloud storage concepts mean that data can be accessed from diverse end devices, possibly by diverse users, i.e., changes can also be made. The increase in digital information is inevitably accompanied by the growing importance of digital evidence. Communication takes place via the Internet, be it via services such as Facebook or Twitter, be it via forums - and of course via e-mail. Cell phones can be tracked; by dialing into radio cells, movements or whereabouts can be traced. All of this information can be relevant to criminal proceedings and can therefore be considered as evidence. Alibis can be verified or falsified, motives can possibly be traced, and connections between people can also be traced. Because of this, consideration of digital data as evidence is not only warranted, but practically unavoidable. In addition, the effort required for monitoring is often considerably less, since the data is collected and preserved either by the persons concerned themselves or by the service providers.

The epitome of criminal proceedings is the establishment of truth by means of the reconstruction of the actual events, which can only succeed if all available evidence is

[6] *Momsen/Rennert*, Big Data-Based Predictive Policing and the Changing Nature of Criminal Justice - Consequences of the extended Use of Big Data, Algorithms and AI in the Area of Criminal Law Enforcement, KriPoZ 2020, pp. 160 – 172, https://www.jura.fu-berlin.de/fachbereich/einrichtungen/strafrecht/lehrende/momsenc/mitarbeiter/momsen_carsten/momsen-rennert-big-data-based-predictive-policing-and-the-changing-nature-of-criminal-justice.pdf.

[7] Cf. already *Endicott-Popovsky/Frincke*, p. 364 ff. in: Schmorrow/Reeves (Eds.), Augmented Cognition, HCII 2007.

recognized and properly evaluated. [8] Digital data have considerable potential to change various forms of communication[9]. Since criminal proceedings are of course nothing other than a specific communication platform[10], these changes also have an impact here. On the one hand, the evaluation of e-mails and communication data from so-called "social networks" has become the central subject of the taking of evidence, and not only in more complex criminal proceedings. On the other hand, to a considerable extent, the initial collection of such evidence is not carried out by members of the criminal prosecution authorities. The 2018 German *Act on More Effective and Practicable Criminal Procedure* expanded the repressive arsenal of investigative authorities standardized in the German Code of Criminal Procedure to include online searches and source tapping. Among other things, this is intended to counter the widespread use of encryption, which often prevents the monitoring of online communications on the basis of existing powers. This form of "digital" law enforcement also and especially covers communication via "social media".

The relationship between the shift of a considerable proportion of communication into virtual space and the state's response in the form of sections 100a (1) sentence 2 and 100b of the amended German Code of Criminal Procedure is not a one-sided one: in view of their scope, the new powers of the authorities are not only of significance for people who must expect to be the focus of criminal prosecution as a result of their own activities. The circle of potentially affected third parties is many times larger than in the case of conventional communication relationships. This is due to the specific nature of communication in social media.

The discussion of what this means for responsible online behavior, even by "normal users," suggests that a basic level of security against becoming the focus of the authorities as a byproduct can be achieved against this background at best at the price of foregoing or significantly restricting communication in social media in a way that runs counter to its nature. Even an "escape" to the darknet, the anonymized and supposedly more secure area of the Internet, does not currently appear to be an alternative for "normal users" because of the increased dangers and limited possibilities it offers, despite the need for anonymized communication channels.[11]

In addition, law enforcement agencies are outsourcing the analysis of secured data to private service providers due to a lack of their own resources.[12] However, law enforcement agencies and their private accessories have to meet the required standards for digital internal investigations, IT/data compliance and data protection law. Nevertheless, from the perspective of German procedural law, the same fundamental questions will have to be asked as with non-digital[13] evidence. In addition to the legal framework for collecting and using evidence, these questions include the value and quality of the evidence as well as

[8] Cf. BVerfGE 57, 250 (275); 63, 45 (61); *Meyer-Goßner*, Einl Rn. 10; § 244 Rn. 11.
[9] In addition with various examples: *Rudolph* in: Akzeptanz des Rechtsstaats in der Justiz, 2013, Materialband zum 36. Strafverteidigertag in Freiburg i.Br. vom 8.-10.März 2013, 2014.
[10] AK-Wassermann, Einl. II, para. 10 ff.
11 The German police, for example, has launched a pilot project "Facebook search," http://www.handelsblatt.com/ politics/germany/ pilot-project-how-police-in-hanover-search-for-witnesses/7382618.html. See Momsen/Bruckmann, Soziale Netzwerke als Ort der Kriminalität und Ort von Ermittlungen - Wie wirken sich Online-Durchsuchung und Quellen-TKÜ auf die Nutzung sozialer Netzwerke aus? (with Bruckmann), KriPoZ 2019, S. 20 ff. (Online and Social Media Searchs), https://kripoz.de/2019/01/15/soziale-netzwerke-als-ort-der-kriminalitaet-und-ort-von-ermittlungen-wie-wirken-sich-online-durchsuchung-und-quellen-tkue-auf-die-nutzung-sozialer-netzwerke-aus/.
[12] For example, at a press conference, the Senator of the Interior of the Federal State of Bremen, *Meurer* (see *Michel* in Weser Kurier v. 6.3.2014, p. 7).
[13] In this respect, the counterpart to digital evidence is not only analog evidence, but also all other evidence that is not based on the perpetuation of information (witnesses, other statements by natural persons).

the scope of the evidence to be presented. The differentiation between the empirical-digital linking fact and the legal assessment of the evidence is also of constant importance. Like a DNA identification pattern[14], a radio cell location can only prove certain facts. On the one hand, the evidence is limited to the fact that a device was switched on in a certain district; in addition, the temporal component (unlike the DNA pattern) results quite precise.[15]

It is much more difficult to determine where exactly the device was located in a possibly very large radio cell with a radius of up to 50 kilometers and a correspondingly large number of individuals who may have been at various specific locations there. Thus, only a probability-based approach to the crime scene is made. Whether a specific person was using the device at the time can only be verified - if at all - with additional evidence, such as fingerprints or witness observations. Only on this basis does the assessment of evidence take place. The temptation to mix factual and legal evidence on the basis of the apparent objectivity of digital evidence and thus decisively shorten the evaluation of evidence is great.

2. Specific Features and Requirements of Digital Evidence in Germany

In all of this, however, it should be noted that digital evidence has some special features that must be taken into account in criminal proceedings. Due to the digital nature of the stored information, it is possible to change or modify it relatively easily and in many respects.[16] It is possible for anyone to change texts created with a computer or to edit images and videos without great difficulty. The corresponding programs are available in part free of charge and offer possibilities for subsequent modification that would in any case not be so easy with a handwritten document or a photograph developed from a negative. This creates a specific uncertainty factor with regard to the correctness of a fact that is to be proven with the respective file. The assignment of digital information to a person can also cause problems.

If, for example, a computer used to commit a cybercrime is used by several people in a family household, a shared flat or in a company, answering the question of the perpetrator may cause considerable difficulties.[17] With respect to internet-related offenses, there is no sufficient suspicion against the owner of the connection solely on the assignment to his or her IP address. This is because the specific perpetration of a particular person cannot be determined in this way.[18] In the light of the presumption of innocence this evidence alone cannot justify an indictment. The difficulties increase even more if the users use

[14] *Momsen/Weichert*, From DNA Tracing to DNA Phenotyping – Open Legal Issues and Risks in the new Bavarian Police Task Act (PAG) and beyond, Verfassungsblog May 15th, 2018, https://verfassungsblog.de/from-dna-tracing-to-dna-phenotyping-open-legal-issues-and-risks-in-the-new-bavarian-police-task-act-pag-and-beyond/.

[15] *Momsen/Rennert*, Big Data-Based Predictive Policing and the Changing Nature of Criminal Justice - Consequences of the extended Use of Big Data, Algorithms and AI in the Area of Criminal Law Enforcement, KriPoZ 2020, pp. 160 – 172, https://www.jura.fu-berlin.de/fachbereich/einrichtungen/strafrecht/lehrende/momsenc/mitarbeiter/momsen_carsten/momsen-rennert-big-data-based-predictive-policing-and-the-changing-nature-of-criminal-justice.pdf.

[16] *Gercke,* Der unterbliebene Schritt vom Computer- zum Internetstrafrecht, AnwBl 2012, 709 (713).

[17] Vgl. *Casey,* Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, Summer 2002, Volume 1, Issue 2, S. 2; *Chaski,* Who's at the Keyboard? - Authorship Attribution in Digital Evidence Investigations, International Journal of Digital Evidence, Spring 2005, Volume 4, Issue 1, S. 1ff.

[18] Cf. Karlsruhe Regional Court, MMR 2010, 68; Cologne Regional Court, decision of October 20, 2008 - 106-5/08, juris; MMR 2009, 291; Saarbrücken Regional Court, K&R 2008, 320; mostly cases involving requests for inspection of files.

anonymization software, which is frequently and urgently recommended from the point of view of IT security, which can lead to a systematic devaluation of the digital evidence.[19]

A frequently underestimated feature but as well a risk of using digital evidence lies, as indicated, in its supposed objectivity. This is because digital data generally appear to be free of any subjective influence and not very amenable to individual interpretation by the viewer. However, as will be shown, this is a false conclusion. Unlike their analog counterparts, digital data must pass through one or more intermediate steps in order to be usable at all. Of course, an analog photograph, for example, must also be developed. However, the development of such a photo is a purely chemical process, with the help of which the photographed motif is made visible in its unchanged form.[20] Digital files, on the other hand, require appropriate programs in order to make sense of the information contained in a text, image or audio file; embodiment requires the creation of a printout. Here, it cannot be ruled out that the display might vary depending on the program used - there is no guarantee that a file will be reproduced in the form and completeness corresponding to the one originally created. [21]

Furthermore, the initial collection of evidence, and in some cases even the "creation" of the digital evidence, is often not in the hands of the law enforcement authorities.[22] This creates a more complex and less obvious, but nevertheless significantly higher risk of manipulation and loss of evidence-relevant information than with most conventional evidence.[23] In parallel, there is the problem that the parties – when digital evidence is used - are often confronted with such a high volume of data that a selection process in the sense of a reduction to information that is essential to the proceedings must take place early on in the investigation process. And this selection usually applies to the investigating authorities. Hence, that this step must be comprehensible and verifiable for the other parties, insofar as they are entitled to inspect the files. Admittedly, this often fails in practice due to two circumstances: The volume of raw data, if in the range of several "terabytes", can overwhelm the data processing capacities not only of small or medium-sized law firms. The investigating authorities themselves also face considerable difficulties.[24] So far, there are hardly any elaborate and comprehensible instruments for dealing with "big data" on the part of the investigating authorities; the selection is usually made according to subjective criteria, which makes it very difficult to reconstruct this process, which is constitutive for the taking of evidence.

In addition, the raw data would have to be made available to the parties at a relatively early stage due to the time required for evaluation in any case, if a suspension of the proceedings is to be avoided. With regard to the principle of "fair trial" (Article 6 European

[19] *Meier*, MSchrKrim 2012, p. 198.
[20] Cf. the corresponding Wikipedia entry at http://de.wikipedia.org/wiki/Entwicklung_(film).
[21] As an example only text files are mentioned, for which due to the most different configurations during the creation the PDF format was created for the most uniform reproduction possible, see http://de.wikipedia.org wiki/ Portable_Document_Format.
[22] On the process of evidence creation *Marshall* (fn.1), p. 55 ff.
[23] Cf. *Geschonneck* (footnote 1), p. 243 ff.
[24] It is obvious, however, that the investigating authorities are hardly in a position to cope with the volume of data stored as evidence in a way that is adequate for the proceedings. For example, Interior Senator *Meurer* (Bremen) stated at the beginning of March 2014 that the average "processing time for the evaluation of storage media is between 6 and 12 months. The police union, on the other hand, assumes processing times of up to 36 months. "Overall, you have a huge problem of a practical nature with data evaluation," the interior senator said, and the incoming data volumes are getting larger; "... we are getting slammed with hard drives, not only in the area of child pornography." *Meurer* also reported that in more complex cases, external companies are also used to evaluate the evidence, cf. fn.13 (*Michel* in Weser Kurier v. 6.3.2014, p. 7).

Convention on Human Rights[25]), otherwise it would be all too easy to create grounds for appeal that would be far-reaching. It is obvious in principle that the defense will be adversely affected in the long term if either the raw data are not made available at all or are made available so late that an evaluation, which, as will be shown, often requires the involvement of experts, can no longer be carried out before the information is used in the main hearing.

As already mentioned, the digital file, like the digital data itself, is, apart from a very few special constellations, completely unsuitable as evidence in criminal proceedings conducted according to the principles of orality and immediacy. Both principles are more relevant and formally observed in German or European (civil law) proceedings than under common law. However, digital data must be visualized or otherwise made perceptible by means of a transformation and editing process. This editing process is evidently extremely critical for the quality of evidence. For processing is nothing other than manipulation (in a value-neutral sense); under certain circumstances, one could even speak of the "production" of the evidence in the narrower sense. Both terms are extremely problematic from the perspective of procedural law in connection with evidence.

3. Advantages of Digital Evidence

In addition to the uncertainties mentioned, however, the processes of digitization have probative value in regard to alleged criminal behavior. As easy as it may be to make subsequent changes to files, this does not usually happen without leaving a trace. Just like the original information, the modifications and often even the individual data calls can be traced and proven, for example, via log files or metadata. The fact that this opens the way to what is figuratively an "infinite regress" with regard to modifications of the metadata that are also theoretically possible requires no further explanation. However, manipulations at higher levels usually require significantly greater knowledge and labor resources. Reconstruction of the file quite frequently can exclusively be performed by experts from the field of digital forensics (see III below). The same applies to the recovery of destroyed data. Simply formatting a hard drive is less definitive than burning a letter or a photographic film[26]. And clearly, the internet is less anonymous than many people believe, as the movements of an average user can be tracked.[27] Lastly, like any piece of evidence, digital evidence can also be exculpatory. However, it is often not possible for the defendant to make the necessary effort in this regard, so the principle of fairness must be observed particularly carefully by the courts here, because otherwise the loss or non-recognition of exculpatory evidence is to be feared.

III. Digital Data and Evidence Standards

The confiscated DVD or hard drive is merely a visual object that has no evidentiary value beyond the fact of its existence. Even the circumstances of its discovery are usually reserved for witness evidence. The digitized or digitally stored information, and thus regularly the actual object of evidence collection, requires processing in order to be usable as evidence in criminal proceedings. [28] In many cases, conventional evidence has to be "processed" in order to be used in court. For example, a photograph must be developed

[25] https://www.echr.coe.int/documents/guide_art_6_criminal_eng.pdf.
[26] *Casey* (fn.1), p. 26.
[27] *Casey* (fn.1), p. 29.
[28] See above II.2.

or a telephone recording played back, and ultimately the witness also reports his or her immediate impressions by transforming acoustic or visual perceptions into speech. In many of these cases, the legal side also has only a very basic idea of how the processing procedure is technically designed. Credibility opinions ultimately serve a comparable goal for witness evidence. It is a matter of illuminating the context of the primary information, which itself, however, remains the evidence-relevant datum.

For digital evidence, however, this processing procedure has a decisive special feature: The information made usable always remains in the context of its digital storage. As an example: the printed e-mail is similar to the conventionally developed photo in that in both cases a technical process creates an eye-witness object (possibly a document). With regard to the authenticity of the evidence, it is primarily important that the conversion process (digital data to readable text, negative to image with accurate exposure and color[29]) is technically flawless. To prove this, the person who carried out the processing would have to be called in as a witness, and if necessary also an expert. Concerning the text file, however, the raw data and metadata are still available during regular processes (hereafter simplified as "context data" [30]).

Without this, meaningful proof of authenticity cannot be provided. They must therefore always be collected, as it were, in the background of the information made "perceptible", which represents the evidence in the narrower sense. Thus, a need arises for standards of evidence suitability also for these contextual data[31]; see below. However, if the context data are indirectly relevant to evidence, the question arises whether and to what extent their authenticity is or must be verifiable.

IV. Evidentiary Suitability and Evidentiary Quality of Digital Evidence ("Forensic Readiness")

The term "forensic readiness" used in common law does not fully correspond in translation (readiness for court or trial) to most civil law jurisdictions. However, in our context it is likely to be accurately captured by "evidence suitability and quality". "Forensic readiness" has a broader, proactive content in the sense that information is created, collected, archived and documented in such a way that it can be used in the hypothetical event of a later trial. Keeping this in mind, it becomes important to have the data to identify every person or institution involved in this process. Then it is possible to ensure that the due diligence obligations incumbent upon them have been complied with in the implementation of process sequences. If so, in this respect there is no liability for errors by the company. According to Rowlingson, *forensic readiness* is defined as “the ability of an organization to maximize its potential to use digital evidence whilst minimizing the costs of an investigation".[32] "Forensic readiness" thus fits primarily into the framework of preventive

[29] Illustrated with risks of manipulation or distortion in *Marshall* (footnote 1), p. 75 ff.
[30] Based on "data context", cf. *Marshall* (footnote 1), p. 83, as distinct from the data themselves or the information content embodied in them ("data content", op. cit. p. 69 ff.).
[31] Overview in *Casey* (fn.1), p. 25 ff; *Geschonneck* (fn.1), p. 64 ff; *Rowlingson* (fn.1), 11 ff; *Tan (fn.1)*, p. 1 ff.
[32] *Rowlingson* (Fn.1),S. 1: "A forensic investigation of digital evidence is commonly employed as a post event response to a serious information security incident. In fact, there are many circumstances where an organization may benefit from an ability to gather and preserve digital evidence before an incident occurs" (a.a.O.). *Tan* (Fn.1), S. 1 definiert wie folgt:"Forensic Readiness" has two objectives: "Maximalizing an environments ability to collect credible digital evidence; and 2. Minimalizing the costs of forensics in an incident response".

compliance, which, however, as "criminal compliance" is itself closely linked to aspects of criminal procedure law.[33]

From the perspective of the defense, which is confronted with evidence based on digital data, it should be self-evident that the standards of "forensic readiness" are also adhered to on the part of the law enforcement authorities, as well as documented and disclosed in a comprehensible manner. This should of course also include the relevance criteria applied in the selection of data material as well as the disclosure of the remaining data stock that was considered to have been set aside.

However, the reality of criminal proceedings is miles away from this. Even the request for evidence from an expert specialized in this field is often rejected with reference to the competence of the forensic departments available at the Federal and State Criminal Police Offices. Their competence, however, is not the source of doubt but the inherent risk of partial loss of evidence or of conscious or unconscious interpretation in the selection and transformation of data into evidence. Although not specific to criminal proceedings, "forensic readiness" sets out requirements that, if met, will significantly increase the probative value of the information presented.

From a comparative perspective, it may be useful to look at common law examples from the United States, which could provide a helpful framework for German criminal proceedings. The "*Daubert* criteria," relevant in common law[34] could serve as an example in the absence of a specific test that could be used to determine whether (digital) evidence has the required scientific quality. The U.S. Supreme Court suggested in the *Daubert* decision in 1993 that several factors[35] should be taken into account in order to avoid false positives[36]:

1. theories and techniques used should have been tested by (scientific) experts;
2. these techniques should have been peer-reviewed and published;
3. a verifiable error rate should be known for the techniques used;
4. standards must exist for their application, and
5. do the theories and techniques used enjoy broad acceptance in the relevant research area? [37]

An updated rule of evidence (US Federal Rules of Evidence No. 702) designated as additional criteria in the 2000 amendment to the rule:

1. the independence of the expert,
2. scientific justification of derivations made[38] ,
3. appropriate review of alternative explanations,
4. observance of the scientific care and whether
5, the field of research represented by the expert is at all capable of producing reliable results on the question of proof. [39]

[33] Excerpt on the objectives of compliance *Bock*, Criminal Compliance, 2011, p. 19 ff; *Rotsch*, p. 3 ff. in: Rotsch (ed.), Criminal Compliance vor den Aufgaben der Zukunft, 2013.
[34] Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579 (1993), zum Fall in *National Research Council* (Fn.1), S 90.
[35] *Casey* (fn.1), p. 73 ff; *Ryan/Shpantzer* (fn.1), p. 2.
[36] *For a* detailed analysis, see *National Research Council* (footnote 1), p. 90 ff.
[37] Daubert v. Merrell Dow Pharmaceuticals, Inc, 509 U.S. 579 (1993), 593 et seq.
[38] In der Kommentierung zur Fed. R. Evid. 702 Verweis auf *General Electric*, 522 U.S. (at 146): "that there is simply too great an analytical gap between the data and the opinion proffered", vgl. *National Research Council* (Fn.1), S. 93.
[39] *National Research Council* (fn.1), p. 93 (with further references) - "... that an expert's testimony is reliable where the discipline itself lacks reliability (...)". In view of the rapidly developing field of "digital forensics", this is of

These factors are not exhaustive and do not constitute a checklist or final standard of evaluation in the sense of a "definitive test".[40] The *Daubert* jurisprudence is a further development of the traditional Frye decision of the District of Columbia Court of Appeals from 1923 on the handling of scientific evidence, which still outlines the requirements for scientific experts today (experience, training, anchoring in generally accepted methods and procedures).[41]

If applied consistently, the *Daubert* standards lead, among other things, to the fact that the results of lie detector tests can no longer be recognized as relevant evidence by American courts. Generally, these criteria are familiar to German and European criminal procedural law and can be readily reconciled with the principles of expert evidence in Section 244 (4) of the German Code of Criminal Procedure. [42] In German criminal proceedings, these criteria can become relevant in two ways. On the one hand, the digital evidence could be presented in such a way that it is already demonstrated at the time of its introduction into the proceedings that the data collection took place in accordance with the aforementioned requirements. This would be the ideal associated with "forensic readiness," which is widely implemented, for example, in DNA identification patterns, fingerprints, or blood alcohol measurements. On the other hand, they designate the standards of review of presented evidence by the court or the defense.

However, in order to be able to effectively review a digital piece of evidence for its probative value, it is essential to know the potential weak points. This is because the corresponding request for evidence must meet the requirements of section 219 S. 1 of the German Code of Criminal Procedure and the case law of the Federal Criminal Court and several state supreme courts.[43]

In view of the specifics of digital evidence outlined above, first of all the history of the creation of the evidence is of interest. Evidence relevant to criminal proceedings generally arises in connection with incidents, i.e., any criminal act, even within a company. After a corresponding incident, evidence often arises in different places and in different forms. Only some locations are known at the beginning of the investigation. Digital evidence, for example, can be stored in different media, be it physical storage media such as DVDs or hard drives, or non-physical, such as social networks or cloud storage. Often, the complete picture only comes together when different storage locations of a piece of information are matched.[44]

Depending on the location of storage as well as the knowledge of possible further storage locations, statements can be made about the integrity and authenticity of the digital evidence. "Integrity" means that evidence must be kept and remain "unchanged". The level of integrity should be as high as possible. Doubts may arise, for example, if the evidence collection was not carried out by law enforcement authorities or if the amount of data was drastically reduced.[45] In both cases, the question arises about the presentation of the raw data in order to be able to verify whether corruption or contamination of the data may have

significance that should not be underestimated with regard to the licensing of experts. If necessary, this could be a reason for an additional expert within the meaning of Section 244 (4) of the Code of Criminal Procedure.

[40] Daubert v. Merrell Dow Pharmaceuticals, Inc, 509 U.S. 579 (1993), 593 et seq.

[41] Frye v. United States, 54 App. D. C. 46, 293 F. 1013 (1923).

[42] Cf. *Meyer-Goßner*, StPO, 56th ed., § 244 marginal no. 75 .

[43] BGHSt 1, 29 (31); 6, 128 (129); StV 2000, 180; *Meyer-Goßner* § 244 Rn. 18 ff; SSW-StPO/Sättele § 244 Rn. 82 ff.

[44] Extensively with examples *Marshall* (fn.1), 19 ff., 85 ff.

[45] In detail with examples *Marshall* (footnote 1), p. 19 ff., 43 ff.

occurred.[46] Authenticity means that the evidence is directly the(same) that was originally obtained. In this respect, the principle of immediacy in criminal proceedings is addressed in a material sense. Problems can arise here if digital data has been transferred to other media or other locations before or after the evidence was obtained. Although this does not necessarily mean that the quality of the evidence is diminished, context data (meta or raw data) will often have to be used to ensure authenticity.

If integrity is lost or the level of integrity falls below a certain level, conclusions can only be drawn to a very limited extent. The same applies to authenticity; the guarantee of this criterion also depends on the possibility of identifying the origin of information. This makes it necessary to evaluate derivative information or contextual data. If, for example, there are indications that a hard disk has been "cleaned," the flash memory cache on the hard disk will also be relevant as evidence in addition to the copy of the hard disk.

Furthermore, the digital evidence must be reproducible. The term "reproducibility" means traceability in the sense of a logical chain of derivation of complex evidence or information from simpler evidence or data. Closely related to this is verifiability in the sense of the internal consistency of the digital evidence. For example: Evidence that by its nature is susceptible to manipulation (such as a lot of stored data) acquires a higher probative value if there are parallel strands of evidence that are altogether consistent with each other. For example, if a piece of information is stored identically in different independent storage locations, this indicates a high probative value, since it is unlikely that all storage locations have been tampered with at the same time.

If we take the example of a document that could be edited on a platform by several users at the same time (e.g. "Google Drive"), the probative value increases if different users have saved the document in an identical manner on their end devices. To be considered are :

1. end uses by devices or persons (entities),
2. the environment, restrictions and controls (environment),
3. organization of the relevant IT (organization),
4. infrastructure of buildings, networks, etc. (infrastructure),
5. workflows (activities),
6. (data) processing processes (procedures) and
7. the data itself (data). [47]

The evidentiary value described by the above criteria can be relatively well divided into categories, as *Casey*, for example, has shown with the "Levels of Certainty" developed by him: [48]

CERTAINTY LEVEL	DESCRIPTION/INDICATORS	COMMENSURATE QUALIFICATION	EXAMPLES
C0	Evidence contradicts known facts	Erroneous/incorrect	Examiners found a vulnerability in Internet Explorer (IE) that allowed scripts on a particular Web site

[46] *Marshall* (footnote 1), p. 40 ff.
[47] On the basis of *Marshall*'s "Seven-Element Security Model" (footnote 1), p. 56 ff.
[48] From: *Casey*, http://flylib.com/ books/en/2.57.1.74/1/ - "Levels of Certainty"; see *Casey* (Fn.1), S. 70.

CERTAINTY LEVEL	DESCRIPTION/INDICATORS	COMMENSURATE QUALIFICATION	EXAMPLES
			to create questionable files, desktop shortcuts, and IE favorites. The suspect did not purposefully create these items on the system
C1	Evidence is highly questionable	Highly uncertain	Missing entries from log files or signs of tampering
C2	Only one source of evidence that is not protected against tampering	Somewhat uncertain	E-mail headers, sulog entries, and syslog with no other supporting evidence
C3	The source(s) of evidence are more difficult to tamper with but there is not enough evidence to support a firm conclusion or there are unexplained inconsistencies in the available evidence	Possible	An intrusion came from Poland suggesting that the intruder might be from that area However, a later connection came from South Korea suggesting that the intruder might be elsewhere or that there is more than one intruder
C4	(a) Evidence is protected against tampering or (b) evidence is not protected against tampering but multiple, independent sources of evidence agree	Probable	Web server defacement probably originated from a given apartment since tcpwrapper logs show FTP connections from the apartment at the time of the defacement and Web server access logs show the page being accessed from the apartment shortly after the defacement

CERTAINTY LEVEL	DESCRIPTION/INDICATORS	COMMENSURATE QUALIFICATION	EXAMPLES
C5	Agreement of evidence from multiple, independent sources that are protected against tampering. However, small uncertainties exist (e.g. temporal error, data loss)	Almost certain	IP address, user account, and ANI information lead to suspect's home. Monitoring Internet traffic indicates that criminal activity is coming from the house
C6	The evidence is tamper proof and unquestionable	Certain	Although this is inconceivable at the moment, such sources of digital evidence may exist in the future

V. Individual Approaches to Review of Digital Evidence in Main Hearings

In order not to open the floodgates to procedural obstruction by individual parties to the proceedings, the rules on requests for evidence in German courts will also have to be applied with regard to the probative value of digital evidence. This means that it is not sufficient to justify a request for evidence with the hypothetical possibility of errors in the sense described above. The court must take this into account in its assessment of the evidence and will be able to assume that there is a presumption of proper technical processes if there is no evidence to the contrary.[49]

Without concrete indications that one of the aforementioned requirements has not been met, this would be a mere "random assertion", but not a request for evidence in the formal sense (under German / European law of evidence).[50] Again, it must be pointed out that the parties must be provided with the context data, i.e., raw and metadata (such as log files) and sufficient time to analyze them properly. In addition, there is a strong case for requiring proof of the above-mentioned criteria of evidence suitability and quality from the outset where the chain of evidence is decisively based on digital evidence.

1. Compliance with Integrity Standards

As explained above, uniform standards must be observed as far as possible in order to validate the integrity of a file. In order to preserve the respective file in its original state, the first step should be to create a copy. With the help of the hash value[51] , which in any case can only be manipulated with considerable effort [52], it can be proven at any time that no

[49] Cf. for the common law, *Casey* (footnote 1), p. 62 f. with reference to the UK Law Commission 1997.
[50] *Meyer-Goßner*, StPO, § 244 marginal no. 20; SSW-StPO/Sättele, § 244 marginal no. 89; BGH StV 2011, 1299 (1300).
[51] Cf. with example *Marshall* (footnote 1), p. 48 f.
[52] Cf. Cologne Regional Court, decision of October 20, 2008 - 106-5/08, juris.

change whatsoever has been made to the original file in the course of further investigations. [53] Possible sources of error can be recognized and particularities of the data type and the specific terminal device used have to be analyzed.[54] In case of e-mails e.g., not only the messages that have already been retrieved and downloaded must be searched, but also those that are still on the mail provider's server. If (image) files were recorded or sent with a smartphone, these as well as received short messages may not only be on the internal memory, but also on memory cards.[55]

If law enforcement authorities are dealing with the digital evidence as with "conventional" evidence it must be ensured that as few people as possible process a file. Furthermore all steps of this processing have to documented without gaps. Outsourcing the evaluation of evidence to private service providers can also be problematic from this perspective.

2. Data Backup

These special features of dealing with digital evidence require that "digital crime scenes" be perceived as such from the very beginning of the investigation and treated accordingly. Complete preservation of evidence is indispensable.[56] It is therefore not sufficient to limit the investigation to just one or more end devices, such as a computer or a cell phone, if peripherals exist. Hence, data could as well be manipulated from these devices. However, data can also be found on these. External hard drives and memory cards must be found and evaluated.[57] This also serves to verify integrity, authenticity and traceability.

The data found must be properly backed up, whereby it is advisable to make a complete copy of the data carrier concerned.[58] In this way, further investigations can be conducted on the basis of the entire data stock without the person concerned having to give up the use of the terminal device - a circumstance that is of decisive importance especially for self-employed persons who depend on their computer. However, this presupposes that the seized data must without delay be stored by the investigating authorities with the lowest possible risk of loss. In the case of particularly precarious data, it may be appropriate to make a perpetuation in the form of screenshots.

Then the risk of unauthorized access, either accidental or deliberate, must also be mitigated. Parties to the proceedings as well as third parties may have an interest in manipulating or destroying the data secured for evidentiary purposes. In view of the increasingly professionalized hacking scene, this requires only a very brief, almost surgical intervention. Access to the preserved evidence must be secured in such a way that access by unauthorized persons - both external and internal - can be virtually ruled out. This is imperative, considering that confidential information, ranging from access passwords to online services to trade secrets, may also be present among the data.59

---

[53] Vgl. *Meyers/Rogers,* Computer Forensics: The Need for Standardization and Certification, International Journal of Digital Evidence, Fall 2004, Volume 3, Issue 2, S. 6f.
[54] See *Hercher/Momsen* (footnote 1).
[55] Cf. *Casey/Schatz,* Conducting Digital Investigations, in: *Casey* (fn.1), p. 211f.
[56] Closer to *Hercher/Momsen* (footnote 1).
[57] See also *Casey,* Handling a Digital Crime Scene, in *Casey,* Digital Evidence and Computer Crime, pp. 227ff. (241).
[58] See also *Bäcker/Freiling/Schmitt,* Selektion vor Sicherung - Methoden zur effizienten forensischen Sicherung von digitalen Speichermedien, DuD 2010, 80.
[59] Cf. the BSI's IT forensics guide, pp. 42ff, 89. The guide can be downloaded from the address https://www.bsi.bund.de/ContentBSI/Themen/Cyber-Sicherheit/ThemenCS/IT-Forensik/it-forensik.html.

Of course, third parties may also have a considerable interest in such confidential information. At the same time, access to data that is secured at public authorities apparently tends to be easier to carry out. This is because, unlike the companies themselves, the data - which has not yet been evaluated - is generally secured according to uniform standards, without regard to its sensitivity. In addition, the data often remains unused for long periods of time, so that attacks may not be noticed until much later. In order to ensure the integrity of the log files, it may be necessary to make a second copy of the data carrier, which is not used in the evaluation of evidence but is left in its original state, which would also have to be documented.

If only a fraction of the originally secured data is presented as evidence, it must also have been comprehensibly demonstrated that among the data not used as evidence either the core area of the "right of personality"[60] was not affected or that information relevant to the core area was not viewed and used elsewhere. This of course is a very German concept leading to a much more effective protection of personalized data. But under the rule of the GDPR (European General Data Protection Regulation) standards are reaching same high levels all across the Union.

As mentioned above, the pre-selection of which data and in which order they are to be viewed is therefore even more important than with conventional evidence. The introduction of (above-mentioned) verifiable "big data" concepts will become standard in the medium term. It should be noted that the problem described above is exacerbated if the digital evidence was originally collected as part of an internal company investigation. As private investigations follow the principles of criminal procedures only to a very limited extent.[61]

3. Compliance with German IT Forensics Standards

If, for example, a company has initially carried out an investigation itself, the quality of the resulting evidence will depend to large extent on whether the standards of IT forensics have been complied with. The same applies of course, to external IT services that are commissioned by law enforcement agencies to secure and evaluate evidence. The German Federal Office for Information Security (BSI) has summarized the requirements for a forensic investigation process in the IT sector in a guideline that essentially focuses the special features of digital evidence already described[62] and is comparable to the "*Daubert* standards" in terms of methodology.

Acceptance of methods and steps used is required; these must be described in professional expert circles and generally recognized. When new methods are applied, their correctness must be proven. To ensure credibility, the robustness and functionality of methods must be demonstrably given. Repeatability must be possible; if third parties make use of the tools and methods the same results must be achieved with the same source material. Secured digital evidence must not be altered unnoticed by the investigation itself. It must be possible to prove that integrity has been secured. The choice of methods must make it possible to establish logically traceable connections between events and evidence traces and also to persons. That is how cause and effect might be linked. Finally, complete documentation must be created for each individual step of the investigation process. In addition, there must be complete proof of the whereabouts of digital traces and the results

[60] Cf. *Singelnstein* (footnote 1), 600 ff.
[61] Excerpt from *Momsen*, § 6 B II 2 a (Internal investigations from a criminal procedure perspective) in *Rotsch* (ed.), Handbuch Criminal Compliance, 2014.
[62] See *Hercher/Momsen* (footnote 1). From a technical point of view, however, these requirements must be put into perspective, see *Rudolph* (footnote 1).

of the investigations carried out on them, i.e., the traceability of the "chain of custody" known in the English-speaking world.[63]/[64]

If a review of the history of the evidence shows that the standards have been deviated from without any apparent reason, this can correctly be seen as a concrete indication establishing the right to request evidence (sections 219, 244 German criminal procedural code). The most frequent starting point for casting doubt on the quality of digital evidence is incomplete or missing documentation.

VI. Conclusion

Digital evidence is undeniably changing criminal proceedings in Germany. Even if the procedural principles and structures remain unchanged, complex special problems arise as a result. For example, specific standards must be applicated to a considerable extent in the area of data collection. Above all, the documentation of compliance with these standards is becoming increasingly important. Defining these standards requires clarity of terminology. Furthermore, as data security often deems questionable and manipulation is often difficult to trace, special attention must be paid to the evidentiary value of digital evidence - with implications for the assessment of evidence in the main hearing and its presentation in the verdict, as well as for its review in the appellate instance.[65] In certain cases considerable delays will also have to be accepted if the raw and contextual data existing for the evidence presented has to be made available to the parties for review in order to ensure a fair trial. To considerable extent, this will make it necessary to call in experts from the field of "digital forensics." The use of enticingly effective digital evidence must not lead to a creeping devaluation of procedural rights. Many of these problems are intensified by the use of AI. On the one hand, AI can already be used in the creation of digital evidence. However, the use of AI to interpret digital evidence in criminal proceedings is particularly critical and will be explored further in additional white papers in our series.

[63] IT Forensics Guide (footnote 47), p. 24; cf. also *Casey* (footnote 1), p. 21f.
[64] Detailed Guide to IT Forensics (footnote 47), p. 87ff.
[65] See *Hercher/Momsen* (footnote 1), with further references.