ARTICLE:

The use of historical call data records as evidence in the criminal justice system – lessons learned from the Danish telecom scandal

By **Lene Wacher Lentz and Nina Sunde**

Historical call data records (HCDR) are frequently used as evidence in criminal trials. However, several inherent uncertainties are associated with HCDR data, and, additionally, errors may occur when law enforcement processes the data. In Denmark, processing errors were introduced into HCDR from 2010 until 2019. The Danish authorities are currently reviewing more than 10,000 criminal cases in order to secure a fair trial. This article conducts a socio-technical analysis of the Danish telecom scandal, which shows that, in addition to the processing errors highlighted,[1] sources of error are related to competence, cognitive factors and inadequate quality management.

Introduction

The widespread use of mobile communication entails increased opportunities for law enforcement to secure relevant information that may contribute to solving crimes. Digital communication data in the form of historical call data records (HCDR) are frequently used in criminal trials as evidence. For instance, a search on the term "cell tower" in Norwegian verdicts returns 363 responses from the period 1995-2020.[2] HCDR can shed light on the circumstances of an incident, such as who has been in contact with whom (telephones/telephone numbers), at what time and/or at which location (cell tower/cell).

Although HCDR have been useful, they have also been controversial and contested, due to the limitations and uncertainties associated with the information obtained from telecom service providers.[3]

Before we proceed further in discussing what caused or contributed to error in the telecom scandal, it is necessary to outline how we understand the concept of error. An error may be described in many ways. Here, we relate the term "error" to validity, which we think of as "the overall probability of reaching the correct conclusion, given a specific method and data".[4] Thus, we understand error as the invalid results of a method or a process. Christensen and colleagues discuss error in forensic science and distinguish between different types of error due to the sources they originate from: practitioner error, instrument error, statistical error and method error; in

[1] For example, see the English case of *R v Cahill; R v Pugh* – a summary is set out at 9.90-9.95 in Stephen Mason and Daniel Seng, editors, *Electronic Evidence* (4th edn, Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, 2017), Open Access PDF version in the Humanities Digital Library at http://ials.sas.ac.uk/digital/humanities-digital-library/observing-law-ials-open-book-service-law/electronic-evidence ;see also Harold Thimbleby, 'Misunderstanding IT: Hospital cybersecurity and IT problems reach the courts', 15 *Digital Evidence and Electronic Signature Law Review* (2018) 11 – 32; for the Ruling by the trial judge, see *R v Cahill; R v Pugh* 14 October 2014, Crown Court at Cardiff, T20141094 and T20141061 before HHJ Crowther QC**,** 14 *Digital Evidence and Electronic Signature Law Review* (2017) 67 – 71.

[2] The search was performed with the Norwegian term "basestasjon" in Lovdata Pro: https://lovdata.no/pro/ performed 09 November 2020.

[3] See, for example, Coutts, R. P., & Selby, H. (2016). Problems with cell phone evidence tendered to prove the location of a person at a point in time. *Digital Evidence & Elec. Signature L. Rev.*, 13, 76, and Cherry, M., Imwinkelried, E. J., Schenk, M., & Romano, A. (2011). Cell tower junk science. *Judicature*, *95*, 151.

[4] Christensen, A. M., Crowder, C. M., Ousley, S. D., & Houck, M. M. (2014). Error and its meaning in forensic science. *Journal of Forensic Sciences*, *59*(1), 123-126.

the context of the telecom scandal, the first two are relevant.[5]

Practitioner error refers to a mistake or operator (human) error. It may be random or systematic, intentional or unintended. The Scientific Working Group on Digital Evidence (SWGDE) also refers to tool usage and the interpretation of results as a human error.[6] Every process that involves a human is prone to human error, particularly when the process involves subjectivity, interpretation, judgements and decisions. Examples of human errors are false negatives – they do not find what is actually there – or false positives, where they find or see something that is actually not present. A human may misinterpret the meaning of the evidence. When concluding or presenting the evidence, there is a risk of overstating (or understating) the relevance or reliability of the evidence.

Practitioner error can be mitigated by quality assurance systems, training, proficiency testing, peer review, and adhering to validated protocols and discipline best practices.

Instrument (or technological) error can be defined as the difference between an indicated instrument value and the actual (true) value. These errors may be related to the tools or techniques themselves or to the implementation of the tools or techniques.[7] An error rate may be calculated through testing of the instrument or technology, and error may be minimized by proper maintenance and calibration.[8]

In this article, we will first provide an overview of the Danish telecom scandal. We will outline the measures that were introduced in the wake of the telecom scandal and point out some limitations in relation to these. We then discuss the telecom scandal from a socio-technical perspective, with particular focus on the human factors that may have played a part. We argue that such a scandal may repeat itself in this or other domains if these factors are not taken into account.

The Danish Telecom scandal

Legal framework on the use of HCDR in Danish criminal cases

Since 2007, Danish telecom service providers have been obliged by law to retain data related to telecommunication as regards traffic data (who is communicating with whom and when), the relevant location data, the means of communication used, etc., including certain user information connected to Internet sessions. The telecom service providers are required to keep the data for a year.[9] Although such a retention regime was evaluated as contrary to EU law by the EU Court of Justice in 2016, no changes have been made to the Danish legislation.[10]

In addition to the retained data, the telecom service providers might be in possession of other kinds of telecom data related to their network, for example "signalling data" from mobile units, meaning data generated from the cell towers related to a switched-on mobile telephone that has not actively been used for communication.

In the case of the police wishing to obtain HCDR from the telecom service provider in a specific investigation, this is regulated by the Danish Administration of Justice Act. Basically, a court order is required when the police wish to obtain HCDR from the service providers. However, the conditions and

[5] Error and its meaning in forensic science, pp. 123-124.

[6] SWGDE, 2018. Establishing Confidence in Digital Forensic Results by Error Mitigating Analysis. Version: 2.0 (20. Nov, 2018). SWGDE is the Scientific Working Group on Digital Evidence, based in the USA, and was formed by Federal Crime Laboratory Directors in 1998.

[7] SWGDE, 2018. Establishing Confidence in Digital and Multimedia Evidence Forensic Results by Error Mitigation Analysis. Version: 2.0 (20. Nov, 2018).

[8] Establishing Confidence in Digital and Multimedia Evidence Forensic Results by Error Mitigation Analysis, and Christensen, A. M., Crowder, C. M., Ousley, S. D., & Houck, M. M. (2014). Error and its meaning in forensic science. *Journal of Forensic Sciences*, *59*(1), 123-126.

[9] The Danish Judicial Procedure Act, § 786, and the Justice Department's order no. 988 on 28th September 2006 about data retention.

[10] The Tele2 judgment on 21st December 2016, in the joined cases, *Tele2 Sverige AB* (C-203/15) and *Watson* (C-698/15). See also Digital Rights judgment on 8th April 2014 in the joined cases, *Digital Rights Ireland Ltd* (C-293/12) and *Kärntner Landesregierung* (C-594/12). See Anja Møller Pedersen, Henrik Udsen and Søren Sandfeld Jakobsen: "Data retention in Europe – the *Tele 2* case and beyond", International Data Privacy Law, 2018, Vol. 8, No 2, pp. 160-174.

procedures for obtaining the permit vary. Lenient conditions apply if the police only demand data concerning which cell tower was used by the mobile telephone at a given time (location data), whereas a more strict legal framework applies if the police demand data about which telephone communicated with which telephone at a given time (traffic data). A request for HCDR could relate to two different perspectives: related either to specific known telephones or to a certain place where a criminal offence has taken place and where the police would like to know which telephones were communicating in the area.

The Telecom scandal

On 17th June 2019, the Danish newspapers disclosed the news that the Director of Public Prosecutions had informed the Danish Bar and Law Society and the Danish Court Administration about an error in the police IT system. The error was identified and corrected on 8th March 2019, and the Director of Public Prosecutions had decided that a number of criminal cases from 2012-2019, where HCDR had been obtained, the Directorate of Public Prosecutions ordered a review and the Danish National Police. Subsequently, this news was followed by a number of critical articles from both technical and legal perspectives. The criticism was particularly levelled at the delay and incomplete information provided to the criminal system and the public. As a result of the increasing number of errors and uncertainties discovered in the handling of HCDR and the subsequent considerations, the Director of Public Prosecutions ordered a halt of two months in the prosecutors' use of HCDR as evidence in criminal trials and hearings about preliminary custody. Currently, more than 10,000 criminal cases from the period 2010-2019 are being reviewed in order to establish the implications caused by errors and uncertainties in telecom data used as evidence.[11] According to the District Attorney in Copenhagen supervising the review, the status as at February 2020, is that, of the approximately 10,000 cases, 7,576 cases relate to convictions, and the rest of the cases concern unsolved, serious crime.[12] To date, the Task Force has reviewed 213 convictions. In 38 of these cases, the initial opinion was that telecom data might have influenced the outcome of the trial. However, the conclusion from the prosecution's review was that there were no grounds for reconsidering the conviction in these cases, as no relevant errors had been detected in the telecom data.

The telecom scandal also led to consequences outside Denmark. According to the Nordic Police Cooperation Treaty, the police in the Nordic countries may assist each other in obtaining evidence in criminal investigations. As far as the authors are aware, the following description is limited to what occurred in Norway. The first media reports in Norway came in June 2019. On 29th August, the Norwegian Director of Public Prosecutions instructed the police districts, national police units and state attorneys to identify all the pending Norwegian criminal cases with HCDR obtained from within Denmark. In this letter, the recipients were informed that the system in which the error occurred was not in used in Norway, and that there was no reason to suspect the same errors in Norwegian HCDR.[13] On 15th January 2020, the Norwegian Director of Public Prosecutions sent an update to the same recipients, informing them that only a very limited number of ongoing cases involving Danish HCDR data had been identified, and only a few where further evaluations of possible consequences due to erroneous data were necessary. The recipients were instructed to expand the scope of their evaluations to include closed cases involving Danish HCDR from March 2010 to March 2019. The Director of Public Prosecutions also underlined that the police districts had experienced significant challenges in identifying the cases, due to the lack of registries and limited search functionalities. How many hours this task has entailed is unknown, but, due to the reported challenges, there is reason to believe that it has required a significant workload.

[11] The period in focus was extended, as 2010 was the starting point for the initial use of the police converting software; for which see below.

[12] Mail communications to the authors on 17th and 18th February 2020 from the District Attorney in Copenhagen.

[13] The Norwegian Director of Public Prosecutions (28th August 2019. Possible misinformation in traffic- and location data obtained from Denmark. Identification and review of relevant cases. Riksadvokaten (28 August 2019) Mulig feilinformasjon i trafikk- og lokasjonsdata innhentet fra Danmark. Identifisering og gjennomgang av aktuelle saker. https://www.riksadvokaten.no/document/mulig-feilinformasjon-i-teledata-brukt-i-straffesaker/.

Conclusions on the technical error

The Telecenter, a department under the Danish National Police, acts as the single point of contact between Danish police and the telecom service providers. The telecom service providers have different systems for storing and retrieving information, and information is therefore delivered in several different formats to the police.[14] The telecom service providers are not obliged to use a uniform concept, nor are they paid for the data retention. The different formats result from different needs within each telecom company, related to operating the system and billing the customers. Since 2010, the Telecenter has processed the files from the telecom service providers prior to sending them to the respective police districts. Several of the errors have been traced back to the processing of data at the Telecenter.

From the information given by the Danish Minister of Justice on 3rd October 2019, and on the basis of conclusions from both the internal examinations carried out by the Director of Public Prosecutions and the Danish National Police and an independent external review carried out by the consultancy agency, Deloitte, the technical errors in the system relate to the entire chain from the cell tower registering the data to the transmission of the data to the requesting police unit.[15] The errors can be summarized into three overall categories, set out below.

(1) Completeness: missing rows as a result of processing by police software

The telecom service providers register the HCDR in databases. Following a request from the police, data is retrieved from these databases and delivered in a format based on cells, rows and columns, such as those you find in a spreadsheet.[16] Each communication activity, such as telephone calls, SMS, duration of the call, and cell tower position (first and last cell tower during the conversation), etc., is registered as a row. When converting the rows from the raw data, an error in the police software resulted in the loss of rows and, hence, incomplete HCDR.

The reason for the loss of rows was found in a certain "timer" function in the police IT system, used for converting data into the uniform format. In order to ensure efficient forwarding of the data to the requesting police unit, a timer function was set in the Telecenter's IT system, e.g. one hour. However, the system was not programmed to check whether the processing was complete prior to sending the file, and the result was that the data were sometimes sent to the requesting police unit, even though the converting process was not complete. Occasionally, this resulted in the Telecenter sending incomplete sets of converted data with "missing rows" to the requester.[17]

The implications of such an error would depend on the specific criminal case. In the question of an alibi, it might be catastrophic for a defendant who claimed to have been elsewhere than at the scene of the crime, if the data that could confirm his or her statement was among the "missing rows" in the incomplete HCDRs. Not only would the missing rows cause lack of support for the alibi, but the missing information could also be held against the defendant's trustworthiness, for not being truthful about where he or she was at a certain time.

(2) Errors in the converted data

In addition to the missing rows, several other errors resulting from the process of converting the data were uncovered in the HCDRs. The conversion process also led to alteration of the cell towers' geographical

[14] The external examination carried out by Deloitte, (2019) p. 15, in connection to the Danish Telecom scandal, for which see below. Deloitte identified that the police received 100 different formats of raw data in the period from 2011-2019.

[15] The Minister's information, including the internal and external examinations as Appendices, are available at URL: http://www.justitsministeriet.dk/nyt-og-presse/pressemeddelelser/2019, see: "Justitsministerens reaktion på teledata-redegørelser" ("The Minister of Justice's reaction to the telecom examinations", translation by the authors as information and examinations are only available in Danish). The Deloitte examination was updated with minor statistical corrections on 13th of January 2020; https://vidensbasen.anklagemyndigheden.dk/h/6dfa19d8-18cc-47d6-b4c4-3bd07bc15ec0/VB/82220c78-862d-4735-8bee-9cae5cddee6a?showExact=true#page=84.

[16] For a discussion about the highly significant errors in spreadsheets, see *Electronic Evidence*, xii-xiii 'Business records' and 7.144.

[17] See the internal examination from the Director of Public Prosecutions and the Director of the Danish National Police, 28th September 2019 (Appendix 2), p. 62, and the external examination from Deloitte, 1st October 2019 (Appendix 3), pp. 33 and 47.

coordinates. According to the external examination, the predominant error in the conversion caused a difference in the cell tower position of approximately 220 metres; in a smaller number of requisitions, a deviation of approximately 100 metres was identified.[18] Other errors resulting from this process were found in in- and outgoing conversations, the duration of the calls, and types of service (telephone call, SMS, Internet session).

When the telecom scandal emerged, this reccurring error questions the trustworthiness of telecom data. However, the conclusion must be that this error alone, meaning a displacement of a cell tower of this rather small scale, would rarely have an effect on criminal cases. This should be seen in connection with the general uncertainties about using telecom data as evidence, for which see discussion below.

(3) Errors in raw data

The third category of errors uncovered in the telecom scandal involves errors in raw data from the telecom service providers. This category consists of several types of errors. Some are considered to pose a low risk of problems in criminal investigations, since they could be detected fairly easily. An example of such an error is the switching of geographical coordinates, which would result in the cell tower appearing to be situated far away from Danish territory.[19] Others pose a great risk of providing misleading information in criminal investigations. For example, the telecom service providers store information about the geographical position of their cell towers. However, over the years, some cell towers have been moved to different locations, without updating the information about the new geographical position of the cell tower and the range of its cells.[20] This had already been acknowledged as a problem in 2015, by the Minister of Justice giving a reply on the matter to the Danish parliament.[21] Nevertheless, this problem has probably not been paid the appropriate attention over the years. A few months after the outbreak of the telecom scandal, the Danish newspaper *Politiken* considered the list of cell towers in detail, and compared their registered address and their geographical coordinates. They found significant differences between these two registrations for several cell towers. The biggest discrepancy uncovered was more than 100 kilometres. When discrepancies occurred, they mostly concerned the coordinates, which established the correct position, and, to a lesser extent, the address.[22]

The effect of such a problem is difficult to establish, as the procedures within the Telecenter in the Danish National Police have not clarified this point. It is unclear whether they based their assumptions about the suspect's geographical location on the address or the coordinates, and whether they carried out a control for discrepancies between the two types of location registrations. In any case, the differences in such registrations in specific cases could possibly have been discovered by the requesting police unit and then resolved in cooperation with the Telecenter and the telecom service providers.

Besides the irregularities concerning the cell tower locations, the internal and external examinations have also revealed other types of errors in raw data from the telecom service providers. Thus, calls and SMS are also possible by application of new communication services, VoLTE (Voice over Long-Term Evolution) and VoWiFi (Voice over WiFi). In connection with the examinations, it was revealed that not all telecom service providers had delivered all communication data concerning these new data types.[23] This means that the raw data material provided by the telephone companies without these data would be incomplete.

Apart from these identified errors, it has been pointed out that the vast diversity in raw data is a possible source of error. As part of the external examination, a

[18] The external examination from Deloitte (Appendix 3), p. 55.

[19] The external examination from Deloitte (Appendix 3), p. 39.

[20] The internal examination from the Director of Public Prosecutions and the Director of the Danish National Police (Appendix 2), p. 22, and the external examination from Deloitte (Appendix 3), p. 39.

[21] Reply from the Ministry of Justice on 20th October 2015 to question no. 182 from the Parliament's Legal Affairs Committee, and the internal examination from the Director of Public Prosecutions and the Director of the Danish National Police (Appendix 2), p. 22.

[22] Jakob Sorgenfri Kjær: "Telefejl er endnu værre end antaget"; https://politiken.dk/indland/art7389985/Telefejl-er-endnu-v%C3%A6rre-end-antaget, and "Vagthund ser med alvor på nye telefejl" ; https://politiken.dk/indland/art7406682/Vagthund-ser-med-alvor-p%C3%A5-nye-telefejl, both in Politiken, 27th September 2019.

[23] The internal examination (Appendix 2), p. 66.

statistical comparison was carried out on the raw data formats provided by the different telephone companies. Conclusively, 100 different formats from the period 2011-2019 were identified, with each of the 100 data formats varying in at least one of either: (1) the order of the columns, (2) the terminology in the columns, or (3) the number of columns.[24] Illustratively, 30 different formats for dates were identified.[25]

This diversity and the ever-changing raw data formats represent a significant challenge to the Telecenter. Changes in the raw data format would require a control of whether the interpretation is still valid. To ensure a valid interpretation of the raw data at all times, the software would thus need to be frequently controlled and updated.[26] The external review revealed that only one person at the Telecenter was appointed to this task.[27] The frequent changes to raw data formats entail a risk of error, if the resources or manpower for controlling and updating the system are limited.[28]

In addition to the errors mentioned above, the inherent limitations and uncertainties with HCDR must be taken into account. The HCDR are first and foremost registered for the telecom service providers' business purposes. The data are used for optimizing the telecom service, charging for the services and billing the customers. HCDR are hence not stored for law enforcement purposes and may have limitations and uncertainties that should be taken into account when using these data as evidence about who did what, at which time (and duration), and from which position. HCDR are a product of the service offered by telecom companies, where a unit (e.g. a mobile telephone) communicates with the telecom service provider's network and infrastructure (cell towers, antennas, and devices for collection and storing telecom data). The cell towers have antennas, which cover different areas, named cells. Each cell has a cell identification (cell id) and two traits – coverage and capacity. There are several factors that affect the coverage of the cell, such as – but not limited to – the height of the cell tower, the frequency, power and configuration of the antenna, the vegetation, the surrounding settlement and topography. The capacity is also limited, and when it reaches its limits, the call may be directed to the next cell tower within the coverage area. These limitations mean that it is never possible to state with 100 per cent certainty that a cell phone was at a certain place at a certain time, based on the HCDR.

Organizational and procedural aspects

On 3rd October 2019, on the basis of the internal examination, the Danish Minister of Justice concluded that, within the Danish National Police, there had not been sufficient inspection of the quality of the data and there had not been sufficient documentation and follow up of errors. Consequently, information about known errors and risks related to HCDR had not been systematically sent to the relevant parties dealing with criminal cases. Furthermore, throughout the years, the management's focus on the Telecenter has been insufficient.[29]

Specifically, the internal examination mentions that, within the Telecenter, no written internal procedures and guidelines in relation to handling HCDR have been developed, nor, additionally, has the Danish National Police developed any national guidelines for the Telecenter's and the police units' handling of HCDR and quality control of the data.[30]

In relation to checking the quality of the data, an external examination concluded that, before 2018, no general checking of the quality of the telecom data received from the Telecenter was carried out by the requesting police unit, as there was the overall presumption that the HCDR received were correct and complete, and therefore it was not common practice to check whether data in the converted file were complete.[31]

[24] The external examination from Deloitte (Appendix 3), p. 35.
[25] The external examination from Deloitte (Appendix 3), p. 35.
[26] The external examination from Deloitte (Appendix 3), pp. 37-38.
[27] The external examination from Deloitte (Appendix 3), p. 9.
[28] The external examination from Deloitte (Appendix 3), p. 38.
[29] The information given by the Minister of Justice on 3rd October 2019.
[30] The internal examination (Appendix 2), p. 90.
[31] The external examination from Deloitte (Appendix 3), p. 67.

Since November 2018, the Telecenter has enclosed a guideline for quality control of the data when sending HCDR to the requesting police units.[32] The guideline advises the receiver to compare the number of lines in the raw data with the converted data and to check whether the numbers match.[33]

Importantly, however, the telecom scandal is also related to outdated and insufficient IT systems and software within the Danish police in general, and within the Telecenter in particular. The external examination quite disturbingly states that the outdated technical infrastructure poses a significant risk to the continuing operational stability, meaning to securing the continuing delivery of converted telecom data.[34] Even immediate remedies to the existing infrastructure are considered insufficient; hence, there is a need to implement a new infrastructure, adequate for modern standards.[35]

Actions to be taken according to the Minister of Justice

In his conclusion on the telecom scandal and the way forward, the Minister of Justice presented a list of 13 initiatives:

1. Establishment of a new independent unit, monitoring technical investigative means and evidence.
2. The problems inherent in telecom data must be declared in any court proceedings.
3. Establishment of certification of quality control within the Telecenter.
4. Strengthening the Telecenter with resources and more specialized competencies.
5. Establishment of a new cooperation forum between the police and the telecom industry.
6. Relevant education and improvement of competencies for the users of telecom data.
7. Requesting police units must improve control of the telecom data they receive.
8. Purchasing special equipment to be able to examine the coverage of cell towers in specific places.
9. New guidelines for the deletion of telecom data.
10. Modernization of existing IT systems.
11. Systematic scrutiny of more than 400 IT systems within the police and the prosecution service.
12. Review of IT systems, where technical evidence is stored and processed, e.g. DNA samples and fingerprints.
13. Evaluation and learning from the telecom data incident throughout the Justice Department.

In the following, we limit our discussion to initiatives 1 and 2. The understanding of "an independent unit" (initiative 1), and the handling of inherent uncertainties in telecom data (initiative 2) is discussed below.

The understanding of "an independent unit"

Concerning the establishment of a new independent unit (initiative 1), on 3rd October 2019, the Danish Minister of Justice indicated a need for "a new, independent unit to supervise the process from the time when an investigation goes through a technical process until the time when the results of the investigation are presented as evidence for guilt in a criminal case."[36]

Accordingly, the competence for the independent unit should be to supervise "investigative means" in a broad sense, not only as regards telecom data. However, the focus on an investigation "going through a technical processing" suggests quite a narrow scope, when considering the telecom data case, where, clearly, raw data in itself also present serious errors and uncertainties, even if the police have not exposed the data to any processing or conversion of raw data that the police might perform.

In a draft proposal for new regulation, published on 21st February 2020, the Ministry of Justice suggests

[32] The external examination from Deloitte (Appendix 3), pp. 17 and 78.
[33] The external examination from Deloitte (Appendix 3), p. 78.
[34] The external examination from Deloitte (Appendix 3), p. 7.
[35] The external examination from Deloitte (Appendix 3), p. 7.
[36] Translation by the authors.

the establishment of a new independent unit for the supervision of technical evidence, connected to the Independent Police Complaints Authority. The proposal implies a broad scope for the new independent unit, as the term "technical evidence" is understood as all information, tracks and material gathered to be subjected to a technical examination or process, leading to the presentation of the data as evidence in a criminal trial.[37]

The purpose of the independent unit would be to supervise the development of adequate and relevant procedures and guidelines – and their use by practitioners within the police and the prosecution service – as regards the handling and processing of specific kinds of technical evidence.[38] Furthermore, the supervision would also be carried out in relation to standard declarations, police reports, etc., in order to confirm that reservations and uncertainties related to specific kinds of evidence are appropriately described. In addition, the supervision would concern whether the prosecution in general presents these reservations and uncertainties in connection with the evidence used in criminal trials.

Specifically, the draft proposal emphasizes that the supervision would not aim to verify conclusions from the examination or processing of technical information in specific cases (e.g. whether a DNA match can be verified or whether a person's cell phone has been registered in connection with specific towers, according to the service provider's information) or how these conclusions specifically have been used during the police investigation.

Based on the telecom scandal, the responsibilities given to this independent unit should be carefully considered. Given the importance of digital evidence and our general trust and naivety regarding such evidence,[39] arguments support a quite broad scope for the unit: not only overlooking procedures of conversion, but also the requiring of data in general, taking samples and perhaps even seeking to verify conclusions in specific cases, mapping uncertainties and securing a dialogue and cooperation with the provider of the data, whether private companies or public institutions. We do not know what we might not know in the future, and a constant critical focus on new sorts of data and evidence must be secured.

The conclusion from the statements from the Danish Ministry of Justice must be that the 13 initiatives and the focus by all parties involved within the police, prosecution service and courts are seen as sufficient to "repair" the errors and uncertainties connected with the procedures of acquiring and processing telecom data and thus "repair" the general confidence in the reliability of such technical evidence used in criminal cases.

Understanding telecom data

Recently, new and detailed instructions, from both the Directorate of Public Prosecutions and the Danish National Police, have been produced on the use of telecom data in criminal cases.[40] The overall aim is to secure quality procedures – and the documentation thereof – in both the requiring police units and the prosecution service, when presenting the case and the evidence in court.

As stated in the new Instruction from the Director of Public Prosecutions: In criminal cases, where telecom data is presented as evidence, the prosecutor must verify that all relevant documents are presented. This means that documents must include raw data and, if processing had been carried out, also converted data, besides a report describing the police check of the data quality. Furthermore, a general note developed by Deloitte on general aspects related to the use of telecom data must always be included in criminal

[37] Draft proposal for new regulation, published by the Ministry of Justice, 21st February 2020, p. 33, available at https://hoeringsportalen.dk/Hearing/Details/63761%20. The completion of the regulation concerning the independent unit is now scheduled to be part of the government's program for the parliamentary year 2020/2021.

[38] Draft proposal for new regulation, published by the Ministry of Justice, 21st February 2020, p. 9.

[39] This is comprehensively dispelled in Chapter 6 of *Electronic Evidence* and in Peter Bernard Ladkin, Bev Littlewood, Harold Thimbleby and Martyn Thomas CBE, 'The Law Commission presumption concerning the dependability of computer evidence', 17 Digital Evidence and Electronic Signature Law Review (2020) 1 – 14.

40 "Anvendelse af teledata i straffesager" ("The use of telecom data in criminal cases", translation by the authors), issued by the Directorate of Public Prosecutions on 29th October 2019 (latest update on 3rd of April 2020), at https://vidensbasen.anklagemyndigheden.dk/h/6dfa19d8-18cc-47d6-b4c4-3bd07bc15ec0/VB/dfa9e79e-2c97-4013-81c9-5699a5ffb3ef?showExact=true (only available in Danish).

cases where telecom data are presented as evidence, "with the purpose of securing relevant knowledge with the defence and the court about the potential sources of errors and uncertainties connected to the use of telecom data."[41]

The "Note about the use of historic telecom data in criminal cases", dated 1st October 2019, is developed by Deloitte in connection with the external examination.[42] The note contains a list of the inherent uncertainties related to cell tower data and thus attention points and reservations regarding the use of such data as evidence.

Data can be missing in the data rows presented, for a number of different reasons, e.g. new kinds of data- and communication services, where data are not registered by the telecom service providers in the same way as traditional tele-communications. Also, the selection of which cell towers are relevant can mean that not all data will be put forward, if a mobile unit has used another cell tower for communication.[43]

In this regard, the note emphasizes that HCDR do not show the same accuracy as a GPS system in relation to locating a specific mobile telephone.[44] This highlights the uncertainties surrounding location data for mobile units.[45] First and foremost, it is noted that such data can only be indicative. This is due to a number of different aspects: the landscape, network malfunctions and changes in weather and season, and to which cell tower a specific mobile unit connects ("cell tower jumps".) More specifically, it mentions that fewer obstacles in the terrain lead to a stronger mobile signal; hence, a mobile unit would be able to connect to a cell tower over longer distances across water than over land. In rural areas, there would be fewer cell towers, meaning the telephone (telephone is used for short-hand, but we mean SIM card, or a combination of telephone and SIM card) could "jump" and connect to a cell tower further away. The accuracy of location data can, on one hand, be as close as a few hundred m^2 in closer urban areas and, on the other hand, be extended to several km^2 in rural areas. The applied technologies can also play a role in the range of the cell tower signal. Besides, specific operating conditions can result in errors in the network, with the consequence that a mobile unit at a given time connects to other cell towers than if the network were functioning normally.[46]

Keeping these reservations in mind, the note mentions that telecom data can be used to indicate the location and movements of a specific mobile unit over time. The more connections between a certain mobile unit with a certain cell tower, the more significant the data could be interpreted to be.[47]

Besides telecom data, which telecom service providers are obliged by law to register and keep for a year, the note from Deloitte also elaborates on other sorts of telecom data that the telecom service providers might have and that could be required for specific criminal cases. This concerns "signalling data" from mobile units, meaning data generated from the cell towers related to a switched-on mobile telephone that has not actively been used (called "idle mode" in contrast to "connected mode", where a telephone is communicating either by calls, SMS or Internet connection).[48] There are reservations regarding signalling data, as they are less precise and thus less reliable.[49]

Relating to raw data, the note draws attention to the risk of errors in the registration of cell towers, namely, the insecurity related to the specification of the address of a cell tower, where the coordinates are considered more reliable.[50] In addition, according to recent guidelines from the Danish National Police, establishing the location of the cell tower must not be based on information about the address provided by

[41] Points 1 and 2.4.2 in the Instruction "Anvendelse af teledata i straffesager", ("The use of telecom data in criminal cases", translation by the authors) issued by the Directorate of Public Prosecutions on 29th October 2019 (latest update on 3rd of April 2020), available at https://vidensbasen.anklagemyndigheden.dk/h/6dfa19d8-18cc-47d6-b4c4-3bd07bc15ec0/VB/dfa9e79e-2c97-4013-81c9-5699a5ffb3ef?showExact=true (only available in Danish).

[42] Deloitte Note: "Notat vedrørende anvendelse af historiske teledata i straffesager", (available only in Danish, title translated by the authors), available at https://www.justitsministeriet.dk/sites/default/files/media/Pressemeddelelser/pdf/2019/bilag_4.pdf.

[43] Deloitte Note, point 3.1.2.

[44] Deloitte Note, point 3.1.1.

[45] Deloitte Note, point 3.2.2.

[46] Deloitte Note, point 3.3.

[47] Deloitte Note, point 3.2.2.

[48] Deloitte Note, points 3.1.4. and 4.4.

[49] Deloitte Note, points 3.1.4. and 4.4.

[50] Deloitte Note, points 3.3.

the telephone companies.[51] Instead, the location of cell towers must be based on geographical coordinates of the cell towers, provided appropriate checks have been made, meaning a documentation of the physical location of cell towers, based on observation of the cell tower or material from surveillance.[52]

The Danish National Police emphasize that, despite these new actions to be taken, it will always rely on the participants involved in specific cases – not least the courts – to evaluate how telecom data most appropriately can be presented as evidence, and to what extent further evidence is necessary, in order to verify the specific telecom data.[53]

Socio technical aspects of the telecom scandal

No process involving technology operates in a vacuum. Socio-technical systems thinking is therefore an adequate theoretical perspective to apply in order to understand how the telecom scandal emerged, and how new similar scandals may be prevented. The underlying philosophy of socio-technical systems thinking has remained largely unchanged, but the specific principles and applications have evolved to reflect the changing nature of work, technology and design practices.[54] The emphasis has shifted from an early focus on heavy industry and advanced manufacturing technologies, through to office-based work and services.[55] The common theme across these contexts has been a focus on the introduction of new technologies.

Socio-technical systems theory advocates the consideration of both technical and social factors when seeking to promote change within an organization, whether it concerns the introduction of new technology or when there is a change in the business.[56] Leavitt visualized these as four components (structure, technology, people, task) that should be in harmony.[57] This has been further developed into a hexagon of six interrelated elements (see figure below).

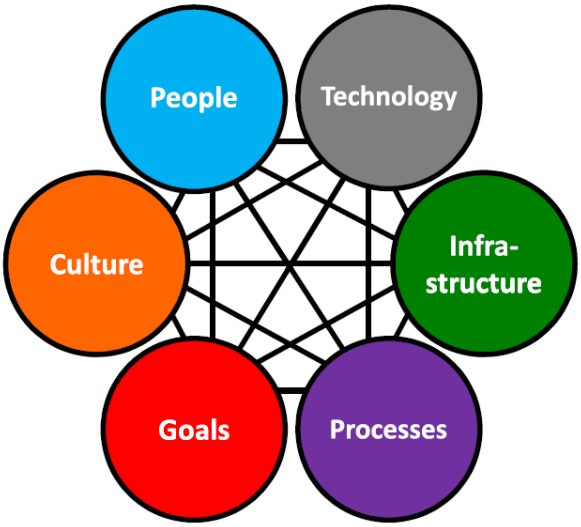

Figure 1: Hexagonal socio-technical systems framework, as described by Clegg and others.[58]

[51] The Instruction "Anvendelse af teledata i straffesager" ("Use of telecom data in criminal cases", translation by the authors), issued by the Directorate of Public Prosecutions on 29th October 2019, with the Appendix 7b: "Rigspolitiets Instruks for politiets anvendelse af teledata til brug for retsmøder under efterforskningen" ("Guidelines from the Danish National Police on the use of telecom data in hearings related to criminal investigations", translation by the authors) on 18th September 2019.

[52] Instruction on the use of telecom data in criminal cases, issued by the Directorate of Public Prosecutions on 29th October 2019, with the Appendix 7b: Guidelines from the Danish National Police on the use of telecom data in criminal investigations, on 18th September 2019.

[53] Considerations from the Director of Public Prosecutions and the Director of Danish National Police, p. 6 in Appendix 1 to the Information given by the Minister of Justice on 3rd October 2019.

[54] Davis, M. C., Challenger, R., Jayewardene, D. N. W., & Clegg, C.W. (2014). Advancing socio-technical systems thinking: A call for bravery. *Applied Ergonomics, 45*(2A), 171-180. doi: 10.1016/j.apergo.2013.02.009.

[55] Advancing socio-technical systems thinking: A call for bravery.

[56] Cherns, A. (1976). The principles of sociotechnical design. *Human Relations, 29*(8), 783-792. doi: 10.1177/001872677602900806

[57] Leavitt, H. J. (1965). Applying organizational change in industry: Structural, technological and humanistic approaches. In J. G. March (Ed.), *Handbook of Organizations* (pp. 1144-1170). Chicago, IL, USA: Rand McNally.

[58] Clegg, C., Robinson, M., Davis, M., Bolton, L., Pieniazek, R., & McKay, A. (2017). Applying organizational psychology as a design science: A method for predicting malfunctions in socio-technical systems (PreMiSTS). *Design Science, 3*, E6.

To work optimally, these interrelated elements must function in harmony. When exploring the factors that may have caused or contributed to error in the telecom scandal, it is necessary to consider all the interconnected elements in a socio-technical system. Covering all will be outside the scope of this article, and we will limit our discussion here to cover people, technology and processes. .

Human error as a cause or contributing factor in the telecom scandal

People play an important role in a socio-technical system, and, when exploring the factors that may have caused or contributed to error in the telecom scandal, we should consider human factors. Here, we will discuss the following aspects as possible sources of error: competence and cognitive factors.

Competence

Identifying, collecting, examining, analysing and presenting digital evidence in a forensically sound manner requires competence.[59] Forensically sound is "The application of a transparent digital forensic process that preserves the original meaning of the data for production in a court of law." [60] There should be documentation of the *continuity of evidence* (also called *chain of custody*) for the evidence, which means documentation regarding where the evidence has been kept at all times and who has handled it.[61] The principle of evidence integrity should be considered paramount, which means that the data should be preserved in its original form.[62] HCDR often require processing in order to derive meaningful information from them in the context of a criminal investigation. This involves splitting up and assembling information pieces,[63] for instance identifying all incoming and outgoing calls from a certain time period from several HCDRs. Any restructuring of data should not result in data being deleted or alter the original data in a way that changes its meaning. Maintaining the evidence integrity of telecom data requires competence in processing the data, assessing the quality, as well as documenting the result.

In relation to the telecom scandal, the Telecenter carried out the process of converting the data into one format. Hence, the Telecenter had the main responsibility for the quality of the product they delivered. As mentioned above, in December 2018, the Telecenter started including guidelines for quality control of the data, together with the raw data and converted data files. Up until this point in time, the police districts had not been instructed or encouraged by the Telecenter to perform any quality control of the data. The new guidelines encouraged the recipient of the HCDR to compare the number of rows in the raw data against the converted data, to assess whether they matched.[64] If performed, this procedure would be an inadequate quality measure, since it would only validate that the files were of a similar size but would reveal nothing about the integrity of the data. Despite the guidelines, the control of completeness was not performed by the police districts. The lack of quality control from the Telecenter and the insufficient guidelines for quality control directed to the police districts demonstrated the inadequate level of competency in handling data at the Telecenter, as well as in the police districts.

Competence is also necessary to derive meaning from telecom data, while taking the inherent limitations into account. Telecom data may appear to be reliable information, since they are accurate and expressed in numeric values. The HCDR data are accurate down to the second; the cell towers are in numeric GPS coordinates. The precise representation of time or place may give the impression that the data is valid, and diminish the attention about limitations and errors. Making valid inferences based on telecom data requires competence regarding why and how the data

doi:10.1017/dsj.2017.4. Image published under a creative commons licence (CC-BY 4.0).

[59] Sunde, N. (2017). Non-technical sources of errors when handling digital evidence within a criminal investigation (Master's thesis, Norwegian University of Science and Technology).

[60] McKemmish, R. (2009). When is digital evidence forensically sound? In *IFIP international conference on digital forensics* (pp. 3-15). Springer, Boston, MA. p. 10.

[61] Casey, E. (2011). *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*. Academic Press, p. 21; for a discussion in the legal context, see *Electronic Evidence*, Chapter 9.

[62] Årnes, A. (2017). Introduction. In A. Årnes (Ed.) Digital Forensics (pp. 1-11). Hoboken: Wiley, p. 6.

[63] Bjerknes, O. T., & Fahsing, I. A. (2018). *Etterforskning: prinsipper, metoder og praksis*. Fagbokforlaget, p. 125.

[64] The external examination from Deloitte (Appendix 3), p. 17.

are collected and stored by the telecom service provider and the inherent limitations of the data. What may be accurate and sufficiently reliable for the purpose of the telecom service provider may deviate from the required quality to serve as reliable evidence in legal proceedings.

Cognitive factors, influences and bias

Regardless of the competence level of the people involved in handling the telecom data, there are other human limitations that may cause error. Cognitive factors and bias affect all processes that involve interpretation, subjectivity, judgements and decisions.[65] Awareness of and understanding about our inherent cognitive limitations and influences that increase the risk of error are essential components for minimizing error. However, awareness is not enough. A necessary step is to identify the particular risk factors for the discipline and implement measures to prevent or uncover any errors.[66] Unfortunately, measures to address cognitive sources of error and bias are often only addressed when scandals appear.[67]

Dr Itiel Dror has focused on cognitive and human error in decision-making within several areas, including forensic science, and has developed a taxonomy of sources that affect the decision-making of forensic experts. These are relevant to handling digital evidence in the context of a criminal investigation[68] and, hence, relevant for handling telecom data. These factors range from the inherent cognitive factors – which relate to how the brain processes information – to external contextual factors that influence the decision-making. Contextual factors may bias decisions, and they are found in the organizational culture and environment, as well as in the particular case. The explanations for why the errors in the Danish HCDRs were not uncovered earlier or why the warnings about error were ignored for such a long time may be found within the levels of this taxonomy, none of which seem to be irrelevant in this respect.

Pohl explains *cognitive bias* as a cognitive phenomenon, which reliably deviates from reality, occurs systematically and involuntarily, and is difficult or impossible to avoid by mere willpower.[69] One fact that may have played a role in the telecom scandal is *confirmation bias*, which can be described as a tendency to seek information that confirms one's belief, and to overlook or explain away information that contradicts it.[70] The receivers of HCDRs believed that the product they received from the Telecenter was of good quality.[71] When the Telecenter (from December 2018) asked the receivers of the HCDRs to control the completeness of the converted data by comparing the number of rows, the receivers (who also believed that the Telecenter provided good quality) would get a confirmation of this notion of quality by comparing the lines in the two spreadsheets, although this would not reveal the true quality of the processed record. It should be noted that the police districts reported that they did not perform this control, since they trusted the Telecenter to deliver data that were accurate and complete.[72]

The same bias may have affected the prosecution authorities. They received a report about the HCDR, often with extracts of the data included. Together with the report, they would also receive the converted HCDR. The prosecution authority checked whether the data included or referred to in the report were consistent with the data from the converted HCDR file.[73] The prosecution authority did not have any knowledge of the insufficient quality control of the converted data file and would probably believe that the data were accurate and complete. If

[65] Dror, I. E. (2017). Human expert performance in forensic decision making: seven different sources of bias. Australian Journal of Forensic Sciences, 49(5), 541-547.
[66] Dror, I. E., & Pierce, M. L. (2019). ISO standards addressing issues of bias and impartiality in forensic work. Journal of Forensic Sciences.
[67] ISO standards addressing issues of bias and impartiality in forensic work , and Cole, S. A. (2016). Scandal, fraud, and the reform of forensic science: the case of fingerprint analysis. W. Va. L. Rev., 119, 523.
[68] Sunde, N., & Dror, I. E. (2019). Cognitive and human factors in digital forensics: Problems, challenges, and the way forward. Digital Investigation, 29, 101-108.
[69] Pohl, R.F., 2016. Cognitive Illusions: Intriguing Phenomena in Judgement, Thinking and Memory. Psychology Press.
[70] Nickerson, R. S., 1998. Confirmation bias: A ubiquitous phenomenon in many guises. Review of general psychology, 2(2), 175-220.
[71] The external examination from Deloitte (Appendix 3), p. 67.
[72] The external examination from Deloitte (Appendix 3), p. 67.
[73] The external examination from Deloitte (Appendix 3), p. 78.

consistency between the report and the converted data file were established, the prosecution authority would have this initial perception of high quality confirmed – even though this measure would not be sufficient to determine the true quality of the data.

The accumulation of bias

Earwaker and colleagues highlight that the failure to acknowledge and to respond to the interlinking nature of participants in criminal justice systems may lead to inappropriate use of evidence in intelligence (or investigative) settings or in court.[74] When a piece of evidence passes through several participants, there is a risk of the accumulation of bias (called in the literature 'bias snowball' and 'bias cascade').[75] The build-up of bias occurs when the effect of contextual information at one stage affects the decision at a later stage.[76] For example, in the telecom scandal, the personnel at the Telecenter believed that the system performed well when processing the raw data. This overconfidence prevented quality control of the performance. When the data were received by the investigator, the investigator received them from someone they believed had specialist competence in assessing the data and trusted that the data were accurate and complete. When the prosecution received the data, they knew from the documentation that the data had been handled in several stages by people with a higher level of competence in telecom data than themselves. They would therefore also trust the data and, through the assessment of the consistency between data in the report and the converted data, this impression would intensify at each stage. The notion of quality could contribute to the decision about charging the suspect, and hence the bias would also pass into the court.

The cumulative effect of bias may affect the decisions made.[77] For example, when the missing lines in the HCDR do not provide the suspect with an alibi (which he actually would have if the raw data were checked), this would lead to a strong belief in the suspect's guilt. This could in turn lead to a more offensive suspect interview, confronting him with the missing alibi. The suspect's behaviour may be due to the strong belief of guilt, underpinned by the HCDR, leading to tunnel vision, where the suspect interview, as well as other ambiguous evidence, would be interpreted to the detriment of the suspect.

Implicit associations about technology and bias

It is relevant to consider how technology affects human decisions. Elsbach and Stigliani suggest three general beliefs about new information technology: It is mysterious or unknown; it is non-human or alien, and it is complex or difficult to understand.[78] Based on these general beliefs, they suggest that we make *implicit associations*, which are attitudes about objects "that are automatically activated by the mere presence of the object".[79] From their analysis of empirical findings, they suggest that people associate new technology with success and with superiority over older technology, and they relate this to the general belief in new information as mysterious or unknown. This may lead to the favouring of newer over older technology.[80]

Elsbach and Stigliani also find empirical support for the assumption that technology endorsed by legitimate others may lead to a perception of the technology as trustworthy and valuable.[81] They suggest that this is to do with the general belief in technology as complex and difficult to understand.

In relation to the telecom scandal, the implicit bias may have played an important role: first, regarding

[74] Earwaker, H., Nakhaeizadeh, S., Smit, N. M., & Morgan, R. M. (2019). A cultural change to enable improved decision-making in forensic science: A six phased approach. Science & Justice, 12.

[75] Dror, I. E., 2018. Biases in forensic experts. Science, 360 (6386), 243. https://doi.org/10.1126/science.aat8443 and Dror, I. E., Morgan, R. M., Rando, C., & Nakhaeizadeh, S. (2017). Letter to the editor—The bias snowball and the bias cascade effects: Two distinct biases that may impact forensic decision making. Journal of Forensic Sciences, 62(3), 832-833.

[76] Earwaker, H., Nakhaeizadeh, S., Smit, N. M., & Morgan, R. M. (2019). A cultural change to enable improved decision-making in forensic science: A six phased approach. Science & Justice, 60(1), 9-19.

[77] A cultural change to enable improved decision-making in forensic science: A six phased approach.

[78] Elsbach, K. D., & Stigliani, I. (2019). New information technology and implicit bias. Academy of Management Perspectives, 33(2), 185-206.

[79] Hewstone, M., Rubin, M., & Willis, H. (2002). Intergroup bias. Annual Review of Psychology, 53(1), 575-604.

[80] Elsbach, K. D., & Stigliani, I. (2019). New information technology and implicit bias. Academy of Management Perspectives, 33(2), 185-206.

[81] New information technology and implicit bias, 185-206.

the introduction of a new system, even though it was not very stable and reliable.[82] Here, we may assume that there was a perception of the new system as being superior to the old and less automated system or method for processing the HCDR. Second, when the members of staff at the Telecenter received the results the system produced, we suggest that they found the new system complex and difficult to understand (only one person was in charge of maintaining it) and trusted the responsible person or the technology to produce reliable and accurate results. And third, when the investigators received the raw file and the processed file from the Telecenter, we may assume that they would also perceive the system converting the data as complex or difficult to understand, and that the members of staff at the Telecenter were the legitimate others that made the result of the processing trustworthy. Each person in the chain represents a layer of trust and, hence, there is a reason for the bias to accumulate through the people involved in the criminal justice system.

Procedures: inadequate quality management

To ensure that the system deserves the trust, any technological system processing data that may be used as evidence in criminal proceedings should be subject to *quality control*.[83] There are several possibilities for error in such a system that could delete, misinterpret or change data; the reliability and validity should, therefore, be controlled on a regular basis.[84] This was identified as one of the contributing factors to the telecom scandal. The system used for converting the raw HCDR was trusted, without performing the necessary regular quality control. The personnel receiving the data at the Telecenter assumed that the system produced reliable and valid results when converting the data. However, the personnel at the Telecenter formed an additional layer of trust, since they were expected to be competent and to have performed quality control. This may explain why the personnel in the police districts did not compare the converted data to the raw data. They trusted the quality of what they received from the Telecenter, even though the Telecenter asked them to control the number of lines in the two files. The prosecution authority was the only body that performed a quality check, according to the external examination.[85] The problem was that they did not receive the raw data, but only the converted data file, upon which the quality check was done. Since the data in the report originated from the converted data file, no inconsistencies were detected. This may have led to a false assumption of quality and hence robustness of the HCDR as evidence in the criminal case.

The system converting the HCDR, the people operating it, and the procedures they followed may be compared to what is framed as Digital Forensics as a Service (DFaaS). The concept originates from a project run by the Netherlands Forensics Institute.[86] DFaaS is described as a "service-based approach for processing and investigating the high volume of seized digital material".[87] Although the concept was described for digital forensics, it is highly relevant as inspiration for the handling of HCDR in the Danish police. Telecom data are also digital, and, although they come in different formats, they do not have the same level of complexity as other digital evidence may have.

In DfaaS, digital information is stored in a central storage facility that purports to guarantee the integrity of the data. Detectives, digital forensic examiners and analysts may obtain access to and explore the data, run queries and visualize results. This service maintains and guarantees the *integrity* of the data, while enabling access in an effective way. Outside such a system, the integrity of digital files should be documented by calculating a cryptographic hash sum. This sum is unique, and, by comparing the hash sum of two files, one may conclude that they are

[82] Holm, J., (3rd December 2013). Server-bommerter forsinkede vigtigt it-system i tre år. (Server flaws delayed important it-system for three years), available at https://www.computerworld.dk/art/229189/server-bommerter-forsinkede-vigtigt-it-system-i-tre-aar.

[83] ENFSI, (2015). Best Practice Manual for the Forensic Examination of Digital Technology, ENFSI-BPM-FOT-01. Version 01 (November 2015).

[84] For example, see Casey, E. (2002). Error, uncertainty and loss in digital evidence. International Journal of Digital Evidence, 1(2).

[85] The external examination from Deloitte (Appendix 3), p. 78.

[86] Van Baar, R. B., Van Beek, H. M. A., & Van Eijk, E. J. (2014). Digital forensics as a service: A game changer. Digital Investigation, 11, 54-62.

[87] Digital forensics as a service: A game changer.

identical. Inside DfaaS, this was handled automatically.

So, how was the integrity of the data handled in Denmark? The raw data were collected and stored, but only in a database and for a limited period of 24 months.[88] The personnel in the police districts could not obtain access to the original data stored in the database but received a file with the raw data, together with a file containing the converted data. To prove the integrity, a hash sum should have been computed from the original raw data file prior to sending it to the police district, or the original file should have been stored with the purpose of a later integrity check. The external review states that, in some police districts, HCDR were archived according to a fixed structure and with full version control.[89] However, the report does not say whether a hash sum was calculated for the original raw data prior to sending it out to the police districts, or whether the police district receiving the file had a routine of performing this procedure. If the original raw data file was deleted by the Telecenter, and no hash sum was calculated and stored, the integrity of the raw data file sent out to the police district could not be proven. According to the external review by Deloitte, the Telecenter did not store the raw data file, which means that there was no reliable source file to compare the converted data with. This means that when the Telecenter asked the receiver to compare the number of rows in the converted data against the raw data file they received, the Telecenter interrupted the continuity of the evidence and "outsourced" the responsibility for quality control to personnel that probably lacked the knowledge and tools to check and maintain the integrity of the data they had received.

Technology or instrumental error

Several of the errors uncovered in the telecom scandal have been articulated as technical errors, for instance that the processing led to missing rows and qualitative change of the data. However, the errors in the telecom scandal (including these) are mainly results of human errors. No machine programs itself, and programming errors, such as the timing function that led to the omission of rows,[90] points back to the human. It is widely recognized that a computer system should undergo regular reliability testing, particularly when changes are made, such as when it has undergone a version update.[91] In relation to the telecom scandal, the validity of the outcome depended on how well the system handled the diverse raw data formats. The external review uncovered 100 different formats of raw data in the period from 2011-2019.[92] This was complicated even further by unannounced format changes by the telecom service providers during this time period. The changes in format introduced a risk of erroneous interpretation of the raw data. Similar to programming errors, failing to update the system – or assessing whether it produces a valid outcome – is a human error. Minimizing interpretation error by updating and validating the system would require human effort. When the total manpower for handling this task, in addition to administering requests for HCDR from the police districts was 1.2 full-time positions, errors were probably unavoidable.

Lessons learned from a human rights perspective

Based on our knowledge of the telecom scandal, we argue for lessons learned in relation to:

> (i) transparency regarding data and procedures that might be presented as evidence in criminal trials;
>
> (ii) securing both data that is as correct and objective as possible from the outset and to the widest extent possible; and
>
> (iii) transparency in respect of the processing of data into another format,

thus giving the suspect an insight into the evidence against him and the opportunity for an adversarial proceeding. As learned from the telecom scandal, even though no intent to cause errors and uncertainties was detected in the system or the

[88] The external examination from Deloitte (Appendix 3), p. 17.
[89] The external examination from Deloitte (Appendix 3), p. 17.
[90] The external examination from Deloitte (Appendix 3), p. 47.
[91] For example https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cftt.
[92] The external examination from Deloitte (Appendix 3), p. 35.

personnel handling the telecom data, the risk of such implications can be built into or hidden in the systems and procedures. As well as witnesses in court being carefully interrogated in order to establish whether they are to be trusted or not, a constant critical review of the specific digital evidence must be maintained.

Such a perspective would correspond with the right to a fair trial, according to article 6 in the European Convention on Human Rights. As stated by the Grand Chamber in *Rowe and Davis v The United Kingdom* (Application no. 28901/95), 16th February 2000, § 60: "It is a fundamental aspect of the right to a fair trial that criminal proceedings, including the elements of such proceedings which relate to procedure, should be adversarial and that there should be equality of arms between the prosecution and defence. The right to an adversarial trial means, in a criminal case, that both prosecution and defence must be given the opportunity to have knowledge of and comment on the observations filed and the evidence adduced by the other party."

The prosecution authorities are obliged to disclose all "material evidence" for or against the accused (see also *Edwards v The United Kingdom* (Application no. 13071/87), 16th December 1992, § 36). This right relates to evidence that is relevant to the decision of the trial and the fairness of the trial as a whole, contrary to material of minor relevance. Furthermore, the Court of Human Rights accepts certain restrictions to this right to material evidence, if strictly necessary to protect specific public interests (*Van Mechelen and others v Netherlands* (Application no. 21363/93 and others), 23rd April 1997, § 58) and provided these limitations to the defence are sufficiently counterbalanced by the procedures applied by the national courts (*Rowe and Davis v The United Kingdom*, § 62).

Digital evidence might "cheat the eye", as the accurate and numerical representations of data appear objective and indisputable, but specifications and details of procedures must be presented for the defence to challenge and perhaps subject to closer scrutiny. The view of the Court of Human Rights on expert witnesses and their statements has been that even though "the domestic judge has a wide discretion in choosing amongst conflicting expert opinions and picking one which he or she deems consistent and credible" in the context of expert evidence, "the rules on its admissibility must not deprive the defence of the opportunity to challenge it effectively, in particular by introducing or obtaining alternative opinions and reports" (*Matytsina v Russia* (Application no. 58428/10), 27th June 2014, § 169). As stated in *Khodorkovskiy and Lebedev v Russia* (Application no. 11082/06 and other), 25th July 2013, § 711: "There is an extensive case-law of the Court which guarantees to the defence a right to study and challenge not only an expert report as such but also the credibility of those who have prepared it, through their direct questioning" (reference made to *Brandstetter v Austria* (Application no. 11170/84 and others), 28th August 1991, § 42, *Doorson v the Netherlands* (Application no. 20524/92), 26th March 1996, §§ 81-82, and *Mirilashvili v Russia* (Application no. 6293/04), 11th December 2008, § 158).

Accordingly, the precondition for a challenge of digital evidence by the defence is the requirement of the prosecution to present the data not simply as columns and figures extracted from a data system. To support the ability of the defence to challenge the evidence, the prosecution must provide a transparent presentation of the data and the processes as a whole, with all the inherent risk of errors and uncertainties. Specifically, there must be transparency concerning the uncertainties that relate to technical and human factors when handling and processing the data. Information about which a specific expert is responsible for the processing must be clear and available, in order to secure the defence the insight and the possibility of cross-examination.

Telecom data or other kinds of data might not always be "material evidence" according to the practice of the European Court of Human Rights, but when the prosecution refers to such data in court as either grounds for investigative measures or evidence in a trial, the details of the data must be presented, in order to secure equality of arms and an adversarial hearing, as part of the right to a fair trial in article 6.

The measures presented by the Minister of Justice indicate a new regime for handling and processing HCDR in criminal investigations. However, without transparency, there is a risk that the measures will not necessarily increase the quality of HCDR evidence but represent several new layers of trust hiding the true quality of the evidence.

Considering the Danish telecom scandal and the thorough scrutiny of the whole chain of gathering,

processing and using HCDR as evidence in criminal trials, there is reason to believe that this subject has been settled for the time being. However, in January 2020, the Danish newspapers broke the news that, in relation to 1,000 customers, a Danish telecom service provider had been delivering the content of SMS communication to the Danish police, who had only presented a court order for signalling data.[93] In February 2020, it was revealed by the press that, since September 2018, in a number of cases, the same service provider had been delivering data related to the recipient telephone numbers from specific communications, in addition to signalling data, even though the police were only presenting court orders for signalling data.[94] The service provider stated to the press that, due to the their IT system, the signalling data were not separated from data related to communication, and the problem had been recognized and discussed with the Danish National Police since March 2019; however, despite insufficient court orders, no halt has been called to the continuing delivering of communication data.[95]

From both a forensic and a legal perspective, a continuing focus on the use of historical cell data records as evidence in criminal cases is constantly relevant and necessary, and the same focus and scrutiny seems highly justified in regard to other types of technical evidence.

Lene Wacher Lentz LLM, PhD is an Assistant Professor at Aalborg University, Denmark. In 2019 she defended her thesis: "The Police's Secret Investigation on the Internet". She has ten years of experience as a prosecutor at the Danish Prosecution Service.

lwle@law.aau.dk

Nina Sunde is a Police Superintendent with 20 years' experience with the Norwegian Police. She holds an MSc in Digital Forensics and Cybercrime Investigation from NTNU/Norway, and is currently a PhD Fellow at the University of Oslo, Norway.

nina.sunde@phs.no

93 Kaare Kronberg Jensen and Jacob Haislund: "Private sms-beskeder delt ved en fejl", in Jyllands-Posten on 26th January 2020, available at https://jyllands-posten.dk/indland/ECE11898353/private-smsbeskeder-delt-ved-en-fejl/, and Kaare Kronberg Jensen and Jacob Haislund in: "Teleselskab: Politiet bad os tie om sms-læk", in Jyllands-Posten on 31st January 2020, available at https://jyllands-posten.dk/premium/indland/ECE11910241/teleselskab-vi-blev-bedt-om-at-tie-i-sag-om-smslaek/. See also Louise Dalsgaard, Henrik Moltke and Marcel Mirzaei-Fard: "Op mod 1.000 danskeres sms'er endte hos politiet: Telenor stod bag fejlen", DR News on 28th January 2020, available at https://www.dr.dk/nyheder/indland/op-mod-1000-danskeres-smser-endte-hos-politiet-telenor-stod-bag-fejlen.

94 Jakob Sorgenfri Kjær: "Telenor har systematisk givet politiet ulovlige teledata siden 2018", in Politiken on 2nd February 2020, available at https://politiken.dk/indland/art7632753/Telenor-har-systematisk-givet-politiet-ulovlige-teledata-siden-2018.

95 Jakob Sorgenfri Kjær: "Telenor har systematisk givet politiet ulovlige teledata siden 2018", in Politiken on 2nd February 2020, URL: https://politiken.dk/indland/art7632753/Telenor-har-systematisk-givet-politiet-ulovlige-teledata-siden-2018.