ARTICLE:

Electronic Evidence in Criminal Procedure: On the Effects of ICT and the Development towards the Network Society on the Life-cycle of Evidence

By **Juhana Riekkinen**

Below is a summary of the doctoral work of Juhana Riekkinen, awarded Doctor of Laws by the Lapin yliopisto (University of Lapland) on 5 June 2019

The development of information and communication technologies and the associated societal development towards the network society, have significantly transformed the context of legal fact-finding. In criminal proceedings, eyewitness testimony and physical tracks and traces used to be the principal forms of evidence. Now, different types of evidence consisting of computer data — i.e. information stored in electronic and digital form, — are increasingly needed in order to prove both online and offline acts and events, with links to suspected crimes. Such electronic evidence is particularly crucial in cybercrime cases, in which eyewitness statements and other traditional types of evidence are not available or scarce because of the digital nature of the offences. However, even traditional crime in the physical world leaves electronic traces in a society where computers and computer networks are ubiquitous, surveillance technologies flourish, and vast amounts of personal data are stored and processed for numerous purposes by countless different private and public organizations.

Thus far, the intersection of law of evidence and information and communications technology ('ICT') has been largely neglected in Finnish legal scholarship. This dissertation aims to remedy this situation by providing an overarching examination of the relevant Finnish law pertaining to different aspects of electronic evidence. An attempt is made to answer two general main questions: (1) *How does the Finnish law of evidence adapt to solving the problems of evidence in the network society?* (2) *What kind of law of evidence is needed in the network society?* The discussion of both questions — which can be divided into numerous sub-questions — is limited to the context of ordinary criminal procedure in the general courts.

The research method employed in this dissertation is, in essence, the interpretation and systematization of applicable legal norms. However, a narrow and dogmatic approach within the traditional confines of law of evidence or procedural law would be insufficient for addressing these research questions. A phenomenon-based and future-oriented approach is needed, and the procedural perspectives need to be supplemented by perspectives from other areas of law, such as legal informatics, criminal law, and constitutional law, as well as from other fields of science, such as sociology, engineering, and forensic science (digital forensics in particular). While a purely comparative approach is not pursued, issues relating to technology are often universal. For this reason, it is useful to look beyond Finnish cases and law, especially when searching for inspiration for possible solutions or legislative improvements. Of particular interest are Nordic and continental countries with similar legal traditions, although insight could also be drawn from some approaches adopted in *common law* jurisdictions.

Because the two initial main questions can be construed as having to do with the quality of law, some measuring stick with which to measure such quality is required. In procedural law, there are certain goals and principles that are widely held to be of fundamental importance in the administration of (criminal) justice. The trial procedure should be sufficiently *certain* in reaching the correct conclusion, both in matters of fact and matters of law. The trial should be as *speedy* and *cheap* as possible. Finally, the trial should also be *fair* to all participants. These goals cannot be achieved by means of law of evidence alone, but it can be posited that the law of evidence — being primarily instrumental, not an end in itself — needs to support the pursuit of these sometimes contradictory, often unattainable aims in the best

possible way. With that in mind, the two main questions can be reformulated as follows: *In the evidential situations of the network society, does the current Finnish law of evidence contribute to certain, speedy, cheap, and fair criminal proceedings? Which measures relating to the law of evidence could be utilized to optimize the certainty, speed, cheapness, and fairness of criminal proceedings in the network society?*

Electronic evidence is a phenomenon that gives rise to various questions, issues, and problems of legal significance. The different, legally relevant aspects relating to electronic evidence can be systematized and contextualized with the help of a life-cycle model. The life-cycle of computer data begins when information with evidentiary value is stored in electronic and digital form (manually, automatically, or through a combination of manual and automated processes). For this data to be used as evidence in a criminal procedure, authorities (or in some cases, private parties) need to locate and collect such data, inspect and analyze them, preserve them until trial, transfer them to other authorities or private parties, and present them as evidence during the trial. After that, evidence needs to be evaluated by the triers of fact. After the evaluation and the judgment in the court of first instance, the evidence may need to be transferred further to the court of appeals to be used in appeal proceedings. The relevant endpoints for the life-cycle of electronic evidence may be permanent archival or deletion. In the present study, the life-cycle model is used to map the different legally relevant problems and to systematize the norms relating to electronic evidence.

The dissertation is structured into seven chapters. In addition to the research statement, chapter I provides a concise overview of the development towards the network society, important fundamental and human rights in the network society, and some general concepts and principles of the law of evidence. Chapters II and III provide some additional context and background information for the following discussion of relevant Finnish law. Some basic concepts and technologies as well as properties and types of computer data and electronic evidence are introduced in chapter II, and the regulation and evidential characteristics of cybercrime are discussed in chapter III. The following two chapters are dedicated to a detailed description of Finnish law pertaining to the collection of evidence from computer systems and networks (chapter IV), and the evidential use of ICT in the courts (chapter V). The discussion is structured according to the life-cycle model mentioned above, with a particular focus on the collection of electronic evidence during the pre-trial investigation, presentation of electronic evidence during the proceedings, and the evaluation of electronic evidence by the triers of fact. Chapter VI contains the analysis relating to the law of evidence and the objectives and principles of criminal procedure, aimed at making the proceedings more certain, speedy, cheap, and fair in the network society. The concluding chapter VII contains some final general remarks.

In Finland, pre-trial investigation is governed by a framework of recent legal acts. For the collection of evidence in particular, the main component of this framework is the Coercive Measures Act (806/2011), which has been in effect since 1 January 2014, having replaced an older act of the same name. The Coercive Measures Act regulates the use of and the prerequisites for the use of coercive measures in criminal investigations, many of which may be used to collect evidence of an offence. Notably, the new act introduced a number of specific provisions on the search and surveillance of digital devices, and reinforced the status of the general principles of proportionality, minimum intervention, and sensitivity. Other relevant components of the framework are the Criminal Investigation Act (805/2011) and the Police Act (872/2011), which entered into effect simultaneously with the Coercive Measures Act. The Criminal Investigation Act governs, as the title suggests, how criminal investigations are conducted, whereas the Police Act contains, among other regulations, powers similar to coercive measures for the purposes of crime prevention and detection. Special provisions on coercive measures and comparable powers are to be found in other legislation. The use of coercive measures is also linked to the material criminal law provisions in the Criminal Code (39/1889), and general procedural and evidentiary provisions found in the Code of Judicial Procedure (4/1734) and the Criminal Procedure Act (689/1997).

The other focus areas of presentation and evaluation of evidence are regulated mainly in chapter 17 of the Code of Judicial Procedure, which has been recently renewed (732/2015, in effect since 1 January 2016). The free theory of evidence, in its Finnish form, guarantees the parties the right to present almost any material as evidence, with no formal requirements for

admissibility. (Exclusion of evidence is possible — but not mandatory — in case evidence has been illegally obtained, as provided in chapter 17, section 25 of the Code of Judicial Procedure.) While hearing of witnesses, experts, and parties is subject to specific rules, the regulation of the presentation of real evidence is almost non-existent. In the 2016 renewal of the law of evidence, almost no attention was given to real evidence in electronic and digital form. The law recognizes two categories of real evidence: documentary evidence, and objects of judicial view. For computer data, this division is not very useful, and the legal classification of certain types of electronic evidence is, at least theoretically, somewhat unclear. The practical implications of this are limited, however. The existing regulation concerning these two categories is very flexible, and largely the same. In practice, the presentation stage is much more governed by the discretion of the presiding judge, and the practical availability of technological means and equipment in the court, than by provisions of written law.

The free evaluation of evidence is the other main component of the free theory of evidence. According to chapter 17, section 1, sub-section 2 of the Code of Judicial Procedure, the court, having considered the evidence presented and the other circumstances that have been shown in the proceedings, determines what has been proven and what has not been proven in the case. The court is to consider the probative value of the evidence and the other circumstances thoroughly and objectively on the basis of free consideration of the evidence, unless provided otherwise in law. In criminal cases, the standard of proof is 'beyond reasonable doubt', and the burden of proof is solely on the prosecutor, as also stated in chapter 17 of the Code of Judicial Procedure. No special guidance regarding electronic evidence or any other types of evidence is offered in the legislation. Further, the case law of the Supreme Court provides very limited guidance on issues specific to electronic evidence.

In relation to the aims of certainty, speed, cheapness, and fairness, the current law of evidence bears both positive and negative characteristics. In the first part of chapter VI, a number of different factors are identified in relation to each objective, and relations between different aims and factors are considered and analysed.

Concerning certainty and fairness, the negative effects are more pronounced than the positive ones. In the environment of the network society, there are considerable risks relating to these aims that are not adequately addressed in the current, rather sparse regulatory framework or legal practice. Of course, electronic evidence is often crucial in reaching a factually correct verdict in a specific criminal case in the Finnish courts, and the current legislation offers wide possibilities for securing various types of electronic evidence relating to criminal proceedings. The law does not directly prevent the appropriate presentation and evaluation of such evidence. However, the current rules regarding collection of electronic evidence, coupled with the lack of specific rules regarding presentation and evaluation, may lead to problematic situations. In the Finnish system, electronic evidence is widely admissible, regardless of concerns relating to authenticity, integrity, and credibility. The rules on the collection and presentation of electronic evidence guarantee neither the quality of electronic evidence, nor that the opposing party and the court receive all the information that is needed for pointing out, recognizing, or testing possible weaknesses and sources of error in this kind of evidence. This lack of transparency may inhibit proper contradictory discussion, and the principle of equality of arms may be in jeopardy. Lack of ICT knowledge and skills may aggravate these problems.

In terms of the other two aims — speed and cheapness — the current Finnish legislation offers plenty of possibilities for utilizing ICT in ways that are suited for preventing unnecessary costs and delays. This applies both to the processing and presentation of evidence that is originally in electronic and digital form, and to the presentation of personal and real evidence with the help of computer systems. Again, the procedural norms leave much to be determined by the parties and the court. Monetary and temporal savings are by no means guaranteed. For evidence-related costs and time consumption in a specific case, the ICT know-how of parties and court personnel, and the availability of suitable technology in the court, and court information systems may be more decisive than the legislation itself.

Finally, in order to find answers to the second main question, an optimization analysis is undertaken in order to identify the best possible means of improving the situation in relation to these aims. Potential remedies for the negative factors and other

improvements are identified and considered. Based on the analysis, ten suggestions are formulated, although it is not possible to offer practical solutions for every problem identified, and, due to the limitations of the research method, some of the suggestions could only be formulated on a rather generic level. The ten suggestions are listed below:

1. Adherence to data protection legislation should be emphasized in the context of securing electronic evidence.
2. Organizations (in particular) should focus on planning how to secure electronic evidence before the offence occurs, utilizing technical measures to provide for the authenticity and integrity of any electronic traces.
3. To improve the quality of electronic evidence, a new provision should be added to the law, obligating the authorities responsible for pre-trial investigation to adhere to any generally recognized best practices in the field of digital forensics, whenever these are not in conflict with specific norms protecting the privacy of an individual or legally privileged relationships (doctor — patient, lawyer — client, etc.).
4. To highlight the importance of the continuity of the evidence (also called chain-of-custody) and the audit trail, a separate provision concerning them should be added to the law, irrespective of the previous suggestion.
5. A specific provision concerning the obligation of the defendant to submit to the use of a biometric identifier in order to bypass a login mechanism or to decrypt encrypted data should be added to the law.
6. The coercive power of extended surveillance should be re-defined in a way applicable to the characteristics of the network environment.
7. A simpler legislative technique should be adopted for defining the offences in the investigation of which different coercive measures are permissible; simultaneously, the conditions of use and definitions for certain coercive measures should be re-evaluated.
8. The need to regulate the presentation of real evidence should be further evaluated.
9. Problems relating to the quality of electronic evidence should be specifically considered when deciding on the admissibility of illegally obtained evidence and in evaluation of such evidence.
10. The basics of ICT and the special characteristics of electronic evidence should be specifically considered in evaluation of evidence, and evaluation should increasingly focus on the processes that have produced the evidence.

As can be observed, many of the suggestions presented here are related to very specific aspects or provisions of Finnish national law concerning coercive measures and pre-trial investigation, and are, thus, mainly of domestic interest (even if some of them are partially inspired by foreign legislative solutions). In contrast, the discussion on how to best evaluate real evidence in electronic and digital form is more universal.

In connection to the suggestions concerning evaluation, a set of auxiliary questions is proposed. These questions have the aim of helping the trier of fact to recognize misconceptions about the meaning or relevance of computer data presented as evidence, and to focus on issues that may have an effect on the evidentiary value of various kinds of electronic evidence (in particular, potential sources of error).

The auxiliary questions include questions related to the origins of the computer data used as evidence. This first subset includes the following questions: *How were the data originally created or how did they come to being? Who or what created the data or input them in a computer system? For what purpose were the data originally created? What roles did manual and automatic data processing play in the creation of the data? What specifically do the data depict or represent, and what conclusions can be drawn directly from them? Which steps lie between the data and their ultimate probandum?*

The second subset concerns the further processing of computer data. The questions in this subset include: *What manual and automatic data processing operations have the data been subjected to before being collected by the authorities, at the time of collection, and afterwards? Have the data been compiled, collated, selected, moved, copied, reformatted, or transformed during their life-cycle, and how have these operations been performed? What technical, physical, organizational, and other security measures have been employed in order to guarantee the authenticity and integrity of the data during their life-cycle? How have different data processing events been documented? Can an unbroken chain-of-custody be established reliably?*

The third and final subset directs attention to the content of computer data, as well as the relations between the content and other material available at trial, and between the content and general background knowledge. Among these questions are the following: *Is the message, document file, media file, or other file consisting of computer data externally whole and intact? Is the textual or observable content generally believable? Is the content internally consistent? Is the content consistent with metadata included in or associated with the data? Is the content consistent with other evidence? Are the data independent in relation to concurring evidence, or have they been produced by an essentially similar (or the same) process? Is there a credible explanation for the internal and external inconsistencies related to the data?*

Due to the nature of electronic evidence, focusing solely on the 'end product' — i.e., the immediately observable textual or audio-visual content of a computer file or printout presented in legal proceedings as such — is unlikely to provide an objective and rational basis for evaluation. Together, the proposed auxiliary questions direct attention towards the life-cycle of data that are used as evidence, and encourage the trier of fact to consider the entire informational process that has led to this evidence being presented in court. The questions have a connection to the presentation stage, as parties could and should try to provide sufficient answers to these questions while presenting and commenting on the evidence, using the questions as a support tool for a contradictory discussion on electronic evidence. Further, asking and answering these questions provides a framework for a well-founded written judgment on factual issues.

These questions do not provide an automatic check-list that must be used in the evaluation process, or free the judge from rigorous thinking and reasoning. The auxiliary questions are not designed to replace any of the existing models or methods of evaluation, but to complement them. It should be noted that the construction of a general method of evaluation or theory of evidence was not pursued in the course of this study. The auxiliary questions may just as well be applied to test hypotheses, rank explanations, or adjust mathematical probability values. However, in the author's view, reasoning based on hypotheses or explanations shows more promise than probabilistic models, especially in evidentiary scenarios typical of the network society. This matter, like many specific questions related to electronic evidence and its legal treatment in various stages, needs to be further investigated.

Juhana Riekkinen, *Sähköiset todisteet rikosprosessissa. Tutkimus tietotekniikan ja verkkoyhteiskuntakehityksen vaikutuksista todisteiden elinkaareen* (Helsinki: Alma Talent 2019), XXII, pp 597 ISBN 978-952-14-3858-5

https://lacris.ulapland.fi/en/persons/juhana-riekkinen%289ce3ca2b-d511-4b2e-b8c4-515d8d074601%29.html