De betrouwbaarheid van elektronische gegevens als bewijsmiddel in het Nederlandse, Duitse en Amerikaanse civiele bewijsrecht

van Stekelenburg, M.C.

2010

document version
Publisher's PDF, also known as Version of record

Summary

The better byte in the battle to be right

The reliability of electronic data as evidence under Dutch, German and American civil law of evidence

Chapter 1
This thesis researches the probative value of electronic data as evidence in Dutch, German and American civil law of evidence. With the introduction of electronic means in the economic and social course of business, electronic data has entered the courtroom as a form of evidence. This causes courts to value and weigh this evidence on its quality and its trustworthiness, despite their lack of knowledge as to the precise risks of electronic evidence a reliable source of the truth.

The main research question in this thesis is: which concrete criteria in Dutch, German and American civil law of evidence are set to electronic data with regard to safeguarding the trustworthiness of these data to prove the facts provided by parties; and which abstract criteria do developers need to take into account when developing new technologies in order to provide for the reliability of the processed and executed electronic data so it can be used as evidence. This research question is twofold. First, I research the concrete criteria which are set by law and precedent to assess electronic data as evidence. Second, by using the answer of the first question as input, I research the more abstract criteria which can be derived from the concrete criteria.

The main concept in this thesis is *to prove*. As a complicating factor Dutch, German and American law have different legal definitions of *to prove*. This does not have to be a difficulty. The assessment of the reliability of evidence is of a factual nature. In this thesis I make an assumption: there is a common understanding on the question when evidence is trustworthy or not and that the courts in the Netherlands, Germany and America are aware of the same risks when weighing the evidence. Indications hereto can be found in the fact that the same kind of legal cases lead to the same kind of outcomes based on the same kind of findings in mainly German and American jurisprudence. Under Dutch law the court need to have become a reasonable extent of certainty (*redelijke mate van zekerheid*). Under German law § 286 ZPO is applicable. The

judge has to make a decision if a fact is true or not true based on due regard of the whole content of the treatise and the conclusions of observation of evidence based on the judge's discretionary conviction. Under American law the preponderance standard of evidence is applicable. The court needs to find that the existence of a fact is more probable than its nonexistence.

Chapter 2

In chapter two the object of research, electronic data, is specified and put into context. Electronic data are facts, concepts or instructions which are stored electronically and which are suitable for communication, interpretation, processing or execution by humans or by automatic means. The smallest building blocks of electronic data are signs. These are symbols, (alphanumeric) characters and other shapes by which data can be represented and processed. Both signs and data are objective. Data can form information when it is interpreted and meaning has been given to it. The human factor of giving meaning to the data makes information subjective.

Electronic data can consist of code and data (in strict sense). Code consists of instructions recorded electronically and which are suitable for initiating, maintaining and ending a process by an automatic means. Data in strict sense consists of facts and concepts (not the instructions though) which are stored electronically and which are usable for communication, interpretation, processing or execution by humans or by automatic means. The justification for the distinction is the difference in function. Code consists of execution rules for a machine which are the instructions for a machine's behaviour. Data on the other hand contains information only. Another argument which justifies the distinction into code and data is the qualification of *geschriften*, *elektronische Dokumenten* and writings. On the other hand the distinction of code and data is not always very clear. Sometimes code is part of data (for instance source code, although without compilation or interpretation this code is not executable) or data is part of code (for instance in print commands)

Chapter 3

Chapter three is on the security of electronic data. The main right to be protected is the right "to prove", the authenticity and the integrity need to be safeguarded. Authentification and integrity relate differently in computer science and legal science. In computer science authentification relates to people (legal subjects) and integrity relates to data (legal objects). Safeguarding authenticity is possible by proving the identity of a person. Computer science distinguishes three classic means to authenticate a person, namely: something a person knows (password, login code), something a person possesses (ID-card, RFID-chip) and something a person is (DNA, fingerprint, voice). Safeguarding the integrity of data is possible by using cryptographic hash functions,

symmetric encryption, a-symmetric encryption, double a-symmetric encryption or a combination of several kinds of encryption.

Chapter 4

Chapter four researches the reliability of electronic data under Dutch civil law of evidence. The probative value cannot be researched without researching the procedural mechanism of the court. Main principle is the passiveness of the court and the autonomy of the parties. The parties decide the scope of the dispute and the court is not competent to complete the legal facts; only the legal grounds can be completed by the court. The autonomy of the parties is limited by legal presumptions. The law or an agreement sets rules with regard to the probative value of legal facts. In this research the legal presumption of the method of authentication of the electronic signature is of importance. A second important principle is the theory of freedom of evidence. This theory holds two mean ideas. First, the open system of the admission of evidence, which entails that all evidence is admissible unless the law stipulates differently. Second, the freedom of the court to weigh the evidence in its official capacity. If jurisprudence is researched for grounds why evidence is trustworthy or not, there are hardly any grounds to find. Though electronic data has been accepted as evidence to prove facts, the reasons why are hardly made explicit in legal decisions. The reasons could be found in the limited obligation to motivate evidentiary decisions or the procedural mechanism of the court. This makes it harder to retrieve the criteria the court based its decisions on to weigh probative value of the evidence. The little jurisprudence available concentrates on the question who needs to prove what and by what means whether an e-mail has been received. The courts are clear and speak with one voice: when a party denies he has received the e-mail, the sending party has to prove that the receiving party has actually received the e-mail. Only in one case the court explicitly motivates why it is convinced the e-mail has been received:

- the sender has received an e-mail which was sent from the same e-mail address as where it has sent an e-mail before.
- the sender has received an e-mail with the same reference as the e-mail it sent before.
- the sender has received an e-mail with content which can only be understood as a response to the e-mail it sent before.

Both the open system of the admission and the freedom of court to weigh the evidence have exceptions. An important exception is the electronic version of the deed. This can be constituted by signing an agreement in electronic form (art. 6:227a BW) in combination with an electronic signature (art. 3:15a BW). De equivalence set in art. 6:227a BW opens the possibility to meet the legal criteria of writing by a document in electronic form. Art. 3:15 BW treats the electronic signature equal as the handwritten signature if the method of authentication is reliable enough. This reliability is determined by the purpose the electronic signature was used for and all other circumstances of the case.

Nevertheless the method of authentication is reliable when it meets six criteria. In that case the law prescribes the legal presumption of the reliability of the method of authentification and as a consequence the electronic signature will be treated equal as the handwritten signature. A problem which arises is that the court can, on its own initiative, weigh the probative value of the criteria of 3:15 BW. If the court finds these criteria not trustworthy or rightfully implemented, is can decide the method of authentication is not reliable enough. As a consequence the electronic signature will not be treated equally as the handwritten signature. The electronic deed therefore offers a false certainty.

Another way to influence the evidentiary position of the parties is a contract of evidence. By using this contract parties can regulate the admission of evidence, the weighing of evidence, the burden of evidence for both parties.

Chapter 5

Chapter five researches the German civil law of evidence. This is part of civil procedural law and is codified in the *Zivilprozessordnung* (*ZPO*). Main principles are the passiveness of the court and the autonomy of the parties. Both have found their way into the so called *Maximen* theories. Under current law the focus is on the *Dispositionsmaxime* and the *Beibringungsmaxime*. Exceptions can be found in the law and several legal presumptions. The German law of evidence has a closed system of admission of evidence, called *Strengbeweis*, meaning it only allows certain types of evidence. Only when determining facts which parties agree on and which are not the essence of the case, other evidence is allowed as well. This is called *Freibeweis*. Under *Strengbeweis* five types of evidence are admissible: observation by the court (*Augenscheinsbeweis*), evidence by witness (*Zeugenbeweis*), evidence by expert (*Sachverständigenbeweis*), evidence by deed (*Urkundenbeweis*) and evidence by the parties themselves (*Parteivernehmung*).

After evidence has been admitted the court has to weigh the evidence on its reliability. Based on § 286 *ZPO* the court is free to weigh the evidence. The court needs to be personally convinced of the truth or untruth of the facts. High probability only is not enough. New jurisprudence tends towards a symbiosis of both subjective and objective elements by requiring personal convincement of the juror and objective probability. No jurisprudence on code can be found. Nevertheless there is jurisprudence on probative value of data and especially on the identity of persons. When a person has an account (e-mail/eBay) which does not have any security mechanisms, then it cannot be used to prove the person who is said to have used the account, really is the person who used it. The security standard is not high enough. In cases where more element scan lead to the conclusion who sent a certain statement, really is the person who made the statement, then the court can qualify the data as

having enough probative value. Under these circumstances are: a combination of content, facts which are mentioned outside the electronic correspondence, names under the statement and the knowledge parties have. The probative value does not depend on one element, but increases when more elements in their mutual relationship lead to the conclusion that evidence is reliable enough and has enough probative value to support the stated facts.
A legal exception to the free weighing of evidence is the *Urkunde*. A distinction is made between *öffentliche Urkunden* and *private signed Urkunden*. Before probative value can be admitted, the court has to make sure that there are no defects to the *Urkunde* and a check to make sure the *Urkunde* is real. Another legal exception to the free weighing of evidence is the *elektronisches Dokument*. As evidence this *Dokument* is admitted as evidence by observation by the court. When the probative value has to be determined, and the *elektronisches Dokument* is signed with an electronic signature, then the *Dokument* gets obligatory force. If the *elektronisches Dokument* is not signed with an electronic signature, then the court is free to weigh the *Dokument* on its merits on the ground of § 286 *ZPO*. When code or data is signed with a qualified electronic signature then the rules of the private Urkunde are applicable to the elektronic Dokument. Its formal binding force is then a fact. In case code and date have not been signed with a qualified electronic signature the Judge is free to weigh them on their reliability.

As under Dutch law, also under German law the evidentiary position of the parties can be arranged by a contract of evidence. Contrary to Dutch law, under German law a contract on the probative value (weighing the evidence) is invalid. § 286 *ZPO* prescribes it is the judge's authority to weigh the evidence. Therefore parties cannot interfere by contract. Parties can only regulate the admission of evidence and the burden of evidence.

Chapter 6
In chapter 6 American law of evidence is researched. In contrast to Dutch and German law of evidence, American law of evidence is not just part of civil procedural law, but it has its own place in law. It is applicable to civil, administrative and criminal law. The American law of evidence originated from English law. Over the last centuries it has developed on its own. Still many rules originating from English law of evidence can be found in modern American law of evidence. In 1971 the prevailing rules have been codified and brought together in the Federal Rules of Evidence (FRE).

Trial by jury was and still is of great influence on American law of evidence. This caused a system in which the judge can investigate whether evidence meets certain legal requirements. First after this qualitative investigation, in the phase of admission, the jury can weigh the evidence.

The American law has an open system of admissibility. This means that all presented evidence will be investigated on five qualitative grounds, namely: relevancy, exclusion, hearsay, authentication and best evidence.

Relevancy means that evidence can only be admitted if it has any tendency to make the existence of any fact that is of consequence to the termination of the action more probable or less probable than it would be without the evidence. As it is strongly depending on the facts, this rule does not provide rules what requirements evidence needs to meet under all circumstances.

Exclusion means that under specific circumstances evidence which is relevant can be excluded. The FRE state the exclusivity grounds, namely: if its probative value is substantially outweighed by the danger of unfair prejudice, confusion of the issues or misleading by the jury, or by considerations of undue delay, waste of time, or needless presentation of cumulative evidence". Only on these grounds evidence can be excluded. As with relevancy, it is very dependant on the facts to give criteria which need to be met by electronic evidence.

Hearsay means that no evidence can be admitted when there is no statement other than one made by the declarant while testifying at the trial or hearing, offered in evidence to prove the truth of the matted asserted. De ratio of this rule is that statements done out of court are not reliable by definition. Statements need to be made under oath, in front of the juror and with the possibility to be questioned by the other party. The FRE lists the exceptions to this rule. No problems arise to admit code and computer generated data, because hearsay cannot occur. Data which is generated by humans can be subject to hearsay. In the following situations there is no hearsay:

- the statement has been made immediately after the event occurred and reflects the memory of the witness' knowledge correctly. What must be understood by immediately is not clear. I can imagine this is dependant on the circumstances. In one of the cases 23 minutes after the occurrence of an event was immediately enough to have Rule 803(1) FRE applicable.
- the statement of the then existing state of mind, emotion, sensation, or physical condition (such as intent, plan, motive, design, mental feeling, pain, and bodily health), but not including a statement of memory or belief to prove the fact remembered or believed unless it relates to the execution, revocation, identification, or terms of declarant's will (Rule 803(3) FRE).
- statements which are recorded by a witness and who has insufficient recollection to testify accurately (Rule 803 (5) FRE).
- statements which the business exception applies to: a memorandum, report, record, or data compilation, in any form, of acts, events, conditions, opinions, or diagnoses, kept in the course of a regularly conducted business activity, and if it was the regular practice of that business activity to make the memorandum, report, record or data compilation, all as

shown by the testimony of the custodian or other qualified witness (Rule 803 (6) FRE).
- statements containing market quotations, tabulations, lists, directories, or other published compilations, generally used and relied upon by the public or by persons in particular occupations (Rule 803 (17) FRE).

The authentication rule means that evidence needs to be sufficient to support a finding that the matter in question is what it proponent claims. It needs to be proven that the evidence is what the proponent claims it to be and that it can be proven whom it comes from. There are many ways to authenticate evidence. Rule 901(b) FRE lists examples without being limitative. There are many ways to authenticate evidence and it is depending on the kind of evidence which method of authentication is most suitable. As code and data have different functions these can be authenticated differently. Methods of authentication listed under Rule 901(b) FRE and applicable to code and date are: the *testimony of witness with knowledge (Rule 901(b)(1) FRE), the comparison by trier or expert witnesses (Rule 901(b)(3) FRE), distinctive characteristics and the like (Rule 901(b)(4) FRE), process or system (Rule 901(b)(9) FRE)*. For data the *public records or reports (Rule 901(b)(7) FRE* are of importance. In jurisprudence several methods of authentication have been developed. Most noticeable is the fact that authentication is considered by several characteristics in their mutual relation. Chapter six analyses these characteristics.

Best evidence (Rule 1001 FRE) is a rule which decides that in principle only the originals of writings, recordings and photographs can be admitted. Duplicated and secondary evidence is only allowed to be admitted in case the original can't be submitted and only under the conditions set in the FRE. When it comes to code and data, the best evidence rule does not seem to apply very well, because it is not always clear if code and data can be considered an original, a copy or secondary evidence. Therefore electronic evidence is assessed by the authentication rule rather than the best evidence rule.

The weighing of evidence and the admission of evidence are strictly separated under American law of evidence, because the first is the exclusive domain of the judge and the latter is the domain of the jury. There are no rules applicable to the weighing of evidence. The weighing of evidence is to the jury who is the fact finder (or in some cases this is the judge). Restrictions like legal presumptions as under Dutch and German law of evidence do not exist under American law of evidence.

Contracts of evidence are non-existent under American law of evidence. Although it is not certain, it is possible these contracts are void based on the fact that a juror cannot be bound by a contract between parties.

Chapter 7

In chapter seven the conclusions of this research are drawn. Jurisprudence and legislation make clear that when it comes to weighing electronic data as evidence most attention goes to the authentication of persons. Electronic data is reliable enough when several characteristics are considered. For instance: the name of the signatory, the name of the sender in the (reliable) e-mail address, the name of the sender in the reply address, the usage of a nickname by a person who is known for using that nickname, abbreviations of the name of the sender, specific characteristics of the text a person has written, the content of a message, the actions/behaviour following to a message which is received by a person, a statement data has been received, witness statement of a person who saw the indicated sender actually is the real sender. To prove certain electronic data was sent by a person, one of these characteristics is not sufficient. The exact amount of characteristics is not clear in detail, but in most cases three of these characteristics seem to be sufficient. This seems to be in line with the principle of two factor identification as known in computer security.

Under Dutch and German law evidence can have binding force. Under Dutch law this binding force is material; under German law this binding force is formal. The binding force is applicable to electronic documents signed with a qualified electronic signature. Under Dutch law these documents can be signed with a normal or advanced electronic signature as well.

Evidence can be unreliable. This is the case with electronic data sent from accounts which are don't provide enough certainty what person the data has come from, but also from accounts the user is know, but when it is not certain enough that person has sent the data itself. The other category consists of the reliability of data found on websites.

In some cases it remains unknown what the probative value of electronic data is. Under Dutch and German law it is not clear what the probative value of the normal electronic signature and the advanced electronic signature is.

The most important criterium in this research is authentication. It can be applicable to legal subjects; then it means to prove the identification of a person. If it is applicable to legal objects, then it means to prove the object has not been modified.

In literature is has been defended that it is important to use the most advanced technical mechanisms to avoid legal problems. However in practice judges seem to have no trouble to weigh electronic data as evidence on its reliability and to consider facts proven.

Chapter 8

Chapter eight lists some recommendations to increase the reliability of electronic data as evidence. These are:

- the usage of a qualified electronic signature;
- the usage of an advanced electronic signature;
- the usage of a normal electronic signature;
- the usage of cryptographic hash functions;
- the usage of the name of the sender;
- the used e-mail address;
- the content of an electronic message;
- the usage of confirmation of receipt;
- to work with (automatic) logs;
- the usage of (automatic) back ups;
- the usage of (trusted) third parties.