Probate law

Poullet, Yves

Published in:
The EDI Law Review

Publication date:
1994

Document Version
Publisher's PDF, also known as Version of record

The EDI Law Review **1:** 83–100, 1994.

Probate Law: From Liberty to Responsibility[1]

Some Reflections[2] *on Continental European Law*

Y. POULLET
Director of the CRID (Centre for Data Processing in Law) of the FUNDP, Dean of the Law Faculty, University of Namur, Belgium

Introduction

From one computer to another, with the help of a vast telecommunications network, electronic data fly about ... in complete security one would say: cryptographic and control programs lock up electronic messages more securely than any bank vault. And isn't it easier to forge a handwritten signature than an electronic one?

Add to the technical argument the imperatives of economic management of both companies and public administration: paper circulates slowly, its storage is expensive ... why deprive oneself of the advantages that our computers and networks are capable of delivering?

Finally, the rarity, even the non-existence of disputes leads one to concur in praise of the excellence of our judicial system and its judges, the perfect adaptation of the law to modern technological realities.

Does any question remain to be resolved? Isn't it enough to make one break into the hymn to liberty at this happy juncture and therewith declare the matter closed?[3]

The use of the so-called N.T.I.C. (New Technologies of Information and Communication) in concluding and filing transactions raises a legitimate fear that the three principles upon which probate law depends may be ruptured:

- the principle of complementarity: each of the parties must dispose equally of the means of proof;
- the principle of transparence: each party should be able, by means of the methods of establishment and conservation of the contract, to measure the extent of their legal commitment;

– the principle of permanence: this applies to the contracts support medium, to which each party should at any time be able to refer and which contradicts the inherent volatility of electronic documents.

Does this triple infraction legitimize throwing a cloak of doubt over the whole question of so-called electronic proofs? Certainly not, as we shall show, but a prudent attitude towards them is justified nonetheless.

Our intended aim is to demonstrate that a better understanding of the three key concepts relating to proof, conclusion and conservation of documents, makes possible the acquisition of electronic proof (I) without a major modification in our legislation, but will require, depending on the case, further provisions in the matter of responsibility (II).

1. The Basic Concepts

1.1. Handwriting – Signature – Copy: Three Key Concepts in Probate Law for Transactions

It is banal to remind ourselves that probate law organizes the protection – however partial – of the person to whom one considers oneself to be a creditor. *Against his creditor, the supposed debtor opposes either the absence or a qualitative defect in the 'support' medium upon which the demand is based; he will take advantage of a lack of written accession to the contents of that support, or will finally establish its insufficiency in the matter of authenticity deriving from the way it has been stored with regard to the original.*

In other words, three concepts form probate law, but in two different stages: the concepts of 'support' or '*handwriting*' on the one hand, those of 'adherence' or *signature* on the other, while bearing on the *proof of the conclusion of a contract*; the matter of '*copy*', its *conservation*.[4]

The first step, then, is to see if and at what cost these concepts allow qualification by the term 'electronic'.

At first sight, these three concepts frame the reality of electronic proof: the one who finds himself faced with proof in the form of an electronic document, will either object on the grounds of a lack of quality or reliability on the part of the programs from which the support originates upon which the attempt at proof is based, or contest that he has not carried out the operation imputed to him or, finally, take advantage of the inherent volatility of electronic documents and the hazards involved in their conservation.

In our opinion, a functional conception seems to justify the suggested equivalents.

1.2. Does an Electronic Signature Really Exist?[5]

1.2.1. The Signature as Concept

The term 'electronic signature' is one frequently used, but is it judicially acceptable? A number of countries (Belgium, Denmark, Portugal, Germany) insist upon the necessity of the handwritten signature as a mark by which a person reveals his identity to another. A more functional conception of the signature departs from this rather cramped vision. Accordingly a signature becomes a sign by which a person, firstly, identifies himself as the author of a particular act and secondly, indicates his willingness to adhere to the contents of an agreement to which that signature refers and to which it is appended. In this sense, certain electronic procedures of identification and verification could be recognized as genuine signatures.

1.2.2. The Electronic Signature

Such a signature consists of a series of characters appended to the end of a document. The series is processed according to certain cryptographic procedures and comprises a coded precis of the message and information relative to the date and hour of transmission as well as the identity of both sender and recipient... Beyond this it offers considerable security: if the message transmitted arrives at a third person, he cannot read it for want of the code required to decipher it. Similarly, if an alteration has been made to the message by a non-authorized person, this can be detected by comparing the electronic signature with the document received.

The functional conception of the signature enables us to assign it the following chacteristics. These seem to us to be fulfilled by certain types of electronic signature.

– *The signature must permit the identification of the signatory*

The relation 'signature – signatory' must be unique and absolute: a given signature can only be associated with one single signatory.

Evidently, in the case of computer generated documents, verification of the adequacy of a signature and its pertinance to the signatory can no longer be carried out in a visual manner, as in the case of manuscript signatures. Verification of the relationship 'text – signature' is therefore undertaken by the appropriate computer program, rather than by a human being.

– The signature may not be 'generated' other than by the sender of the document. It must be sufficiently *free from the possibility of counterfeit or imitation*

The handwritten signature is generated by the signatory in such a way as to be, in principle, unfalsifiable and inimitable. However, one can never assure

absolute certainty in this respect. The same may be said of certain electronic signatures.[6]

An electronic signature is designed, either according to the contents of the document, or according to secret information belonging to and held solely by the sender, or according to information common to both sender and receiver which could be public (for example, an algorithm of the signature used, potential parameters,..), or according to a mixture of the various elements mentioned.

a. *Data permitting the creation of an electronic signature must be sufficient for its verification, but insufficient for its falsification.* The methods both of signing and establishing authenticity must be robust, *in order to render practically impossible any attempt to sign in someone else's place.*

b. The 'notarisation' of such signatures (or even their deposition with an 'electronic notary') improves the security of the system, inasmuch as it assures the parties (sender and receiver) of the integrity, source, date and destination of documents, through the intermediary of a trustworthy third party.[7]

– *The appending of the signature must be significant and made directly on the document to which it refers.* It must be attached to the document in a permanent and indissociable manner during transmission.

Above all, the act of signing must be significant. This means to say that the document must be readable and comprehensible, and that signing it must demand a clear and voluntary action on the part of the signatory. This requirement is nothing new, it is equally at home in the domain of 'classic' paper documents as in the world of computer documents where the desired operation appears on screen but must be confirmed by touching a particular key before it can be carried out.

Furthermore, the signature must be made on the document to which it refers. This requirement poses no difficulty for paper documents. A signature appended to a document has no value except in relation to the content of the paper on which it appears and is ineradicable. To respect the condition of inseparability with regard to electronic documents, the document and its signature must form one single unit, stored together on the support medium. This is not always the case. Perhaps, for reasons of accounting, management or security, the signatures require a higher level of privilege to the documents themselves (privilege, in computer terms, is a means of protecting data by according particular rights of access to information stored in the system to particular persons). Consequently, they may be stored separately or on seperate supports, despite the logical paths that unite them.

Can one therefore conclude that an electronic signature is not joined to the document to which it refers? The reply is negative for two reasons. *An*

electronic signature is by definition 'attached to the document' to which it refers and is established 'in direct relationship to its contents'. Consequently, although they may be physically distinct from one another, the signature remains logically dependant on the document.

To adapt the requirement of permanence and indissociability of the signature to 'computer documents', we must make use of methods that guarantee the inalterability of the document concerned, methods which render any interference by way of addition, modification or the suppression of a signature impossible.

– There must be *no delay, either of time or place* between the acceptance of the contents of a document and the actual appending of the signature.

This requirement refers essentially to the creation of a signature. The signatory may not validate with his signature a document that is not in his possession at the time and whose signing is not of itself significant.

Such a demand disqualifies all types of automated or pre-programmed signature and imposes the presence and intervention of a human being in any act of signing. This condition forbids the presence of any intermediary, whether human or not, between the signatory and the document to be signed. This does not, however, in any way prohibit the use of a signature in a telematic network. Basically, once a person decides, for example, to conclude a contract of sale through telematic means, the contract arrives at the buyers via the telematic network and thence to the sellers terminal. From then on, by definition of the signature, it is impossible for either the operator, the buyer, the seller or anyone with access to the network to modify the signed document. This confirms the idea that the condition requiring the presence of the signatory and the signed document only needs to be verified at one single moment in the processing of the document: the actual act of signing.

1.3. Is an Electronic Document a Document within the Meaning of the Law?

1.3.1. The Concept of Document within the Meaning of the Law or 'Instrument'

The notion of a document within the meaning of the law is hardly dealt with by our legislation. The only definition as such is to be found in the German procedural code;[8] *the term 'instrument' covers all forms of 'directly readable expressions'*,[9] *on whichever support medium, whether paper, optical, magnetic or other.* Such a definition, confirmed by other jurisprudence,[10] responds to the concern to admit the varied and numerous procedures for data storage and transmission.

The high value in probate accorded to instruments is explained by their characteristics. They constitute a durable and reliable support upon which

figure signs forming a language. Such a concept is 'open' and its extension is not limited solely to paper documents: the language can be coded, stability extends to the possibility of being, at any moment, produced in the event of litigation, reliabiity is guaranteed by the technical parameters of storage and of transmission, rather than by the quality of paper. Briefly, any document which reproduces the will of a person in a sufficiently durable form and in a way that can be read by means of an appropriate procedure, is recognized as an instrument, rather than solely the setting down of signs on paper. We need, therefore, not be astonished at the audacity of the fiscal administration, which, in that which concerns electronically generated and transmitted invoices, has recognized that: 'in the case of teletransmission, the probative value of documents exchanged, depends essentially on the setting up of technical means which assure to the system a reliability equivalent to that produced by invoices printed on paper, as well as permitting the assimilation of the teletransmitted invoice as an original'.[11]

1.3.2. From Electronic Document to Instrument

If it seems necessary to extend the meaning of instrument, it also seems indispensible to define the security criteria which permit us to class an electronic document as an instrument. These criteria presume the availability of the document on a magnetic support or on paper and foresee the risks in terms of reliability and integrity.

– '*The document should be unalterable*'

To speak of the unalterability of a document is to speak of fraud. This is easy enough in the case of paper documents, but also quickly detected (scratching or recopying an entry leaves traces), while fraud on computer support media will often pass unnoticed and may hardly ever be detected a posteriori.

Preserving the unalterable character of a document necessitates conserving the same unchanged both in content and form.

To preserve the unalterability of the contents of a document (that is to say, to preserve the sense and authentic character of the original document), neither sender nor receiver should be able to alter the content without the knowledge of the other (after all, does not the modification of a text involve the modification of the signature?). Furthermore, no third party should be able to interfere in the sender-receiver relationship by modifying the contents of the document without the knowledge of both parties.

Various authentification techniques are availalable to guarantee the integrity of data.

– *The document should always remain legible through an appropriate procedure*

Documents on paper fulfil this condition by the simple fact of being set down in a language (vocabulary and grammer) and in a symbolic graphic form (writing) accessible to human comprehension. This is not always the case with information carried by computer support media: they are coded and therefore in an illegible form. It is necessary to use the 'appropriate' intermediary, which will present the stored information in a humanly comprehensible form. This new phase presumes various manipulations and therefore presents a danger to security.

Once a transaction has been concluded, the legibility requirement poses a second condition: taking into account the speed of technical evolution, can we guarantee that a support which is currently in common use is going to remain legible and how, at best, can we assure that a particular computer system will stay abreast of this evolution?

– *The document must be clearly identified in place (name and address of the correspondents) and in time (date of drawing-up, transmission, reception...).*

Computer systems permit precise control of the date and hour that a document was drawn up, sent or read. They also assure the identification of correspondants.

– *The document must be durable*

This requirement calls for an examination of therecorded document's physical support medium (magnetic tape, CD ROM, etc.) and of the chances of its eventual degradation over the years. It further implies an analysis of the methods for rejuvenating such a support, thereby raising the essential question of the fidelity of the recordings made by anyone seeking to establish proof through an electronic medium.

In other words, the durability of the document requires a reflection more upon the guarantees for the survival of the contents than for a support medium which can be erased today, regenerated tomorrow.[12]

1.4. Electronic Archives or 'Faithful Copy'

1.4.1. The Copy: From Opprobrium to Recognition

The copy has a traditionally bad press and article 1334 of the Belgian civil code merely translates that suspicion, since it permits the original to be demanded.[13] The poor quality of copies and the risk of manipulation during the process of transcription justify such an attitude.

The organizational and technical securities which now surround electronic archive operations plead for a change of mentality in this respect. The 'original-copy' distinction responds not only to the needs raised by archives, that is to say, the more long term conservation of data, but also to the need

to take into account the intrinsic volatility of electronic documents which are instantaneously transmitted from one memory to another, either for the purpose of transaction, or merely to serve the structural needs of the system. In other words, in that which relates to electronic documents, it is difficult to distinguish the original from the copy, and the opprobrium cast by some legislations raises rather than solves difficulties. The necessity of granting the 'faithful' copy[14] the same force in probate as the original reponds to the sense of unease expressed by businesses as much in their relations with clients and suppliers as with civil administrations. If there must be a change in the legislation, it should concern the value accorded in probate to the way in which transactions are stored, rather than the way in which they are concluded.

The notion of 'copy' and 'faithful' must be defined: 'is constituting a *copy*, a document reproduced on an information support medium from a writing recorded under private signature'. A copy is deemed *faithful* if the originals have been recorded in accordance with such security criteria as have been decided by the authority concerned, that is to say, criteria of integrity and, if necessary, of durability and confidentiality.

1.4.2. The Fidelity of So-Called Electronic Copies

Analysing the 'faithfulness' of a document's copy, also means paying attention to the methods used to restore or rejuvenate support media, to the ways of prolonging the life of a support, as well as to the defects and qualities of paper and computer support media.

Our suggestions on this point verge on a paraphrasing of the very principles recommended by the Council of Europe.

1. Documents stored on computer-related support media must satisfy the following conditions:
   a) of being faithful and durable recordings of an original recorded source document, either by encoding or reproduction. By recording via reproduction is understood the conservation of an original document both in its graphic form and its content. By recording via encoding is understood solely the conservation of the content of a document. Any indelible representation of the original involving an irreversible modification of the support medium is considered durable. This reproduction is of a physical order if made at the level of the document's physical support medium and of a computational or logical order if made at the level of the data processing parameters used to represent the document;
   b) of being drawn-up in a systematic manner without lacunae;
   c) of being made according to working instructions which have been conserved as long as the reproductions or recordings themselves have been in existence;

d) of being carefully conserved, in a systematic order and protected against all kinds of alteration.

2. The following rules must be respected when drawing up the original document:
   a) the work must be overseen by the custodian or trustee of the document or a person designated by the same as responsible representative, who may be called upon to witness to the method by which the recordings have been made;
   b) such recordings must provide for the order of reproduction or encodage to be determined;
   c) the various phases of the recording must be carried out strictly according to the plan drawn up under the working instructions envisaged in 1c);
   d) the recording must be the subject of an official report, stored with the recording, which must contain the following elements:
      - the identity of the system operator responsible;
      - the nature and subject matter of the documents;
      - place and date on which the operation took place;
      - eventual faults which were remarked during the recording;
      - a declaration, signed by the system operator in charge, to the effect that the documents concerned were recorded in a complete and regular manner without alteration; this declatation may be the object of a recording made at the end of documents just drawn up;
   e) the recording must be perfectly legible by the appropriate means and technically satisfying; the fidelity of the reproduction or encoding must be verified before the original is destroyed;
   f) the recording must always be available for consultation by those persons legally entitled to have access to the data which it contains.
3. The following rules apply to systems for the processing of computerized documents:
   a) systems must deploy such security safeguards as are necessary to assure the inalterability of the recordings;
   b) systems must be so organized as to permit the restoration of the recorded information in an immediately legible form.
4. The following rules apply to such programs as are employed in the processing of computerized documents:
   a) the program's documentation, the descriptions of its files and its operating instructions must be directly legible and kept carefully up to date by the person responsible for their safekeeping;
   b) the documents defined in paragraph a) above must be conserved in a communicable form for as long as the recordings to which they refer.

If, for any reason, the recorded data is transferred from one computer support medium to another, the person responsible must give their prior assent.

1.4.3. Conclusion of Section 1: An Equivalence of Principle: From Assertion to Reality

Our intention was to show that an instrument, its signature and its copy are all concepts open to the more or less complete dematerialisation entailed in the drawing-up of electronic documents and signatures.

The equivalence of principle leads to an equivalence in law if, and only if, the parameters for the drawing-up and conservation of electronic documents in fact fulfil the demands derived from the very functionalism of traditional concepts related to probate law. For example, we have described a document under the meaning of the law as a directly legible support medium. In other words its contents must be accessible to human comprehension and should be communicable as such to the person against whose contention one is using it! Not every electronic document meets these requirements. Thus it follows that only certain documents which meet the functional demands of an instrument can be considered as such. The same reasoning is applicable to the signature and the faithful copy.

2. A New Regulatory Approach to Electronic Proof

2.1. A Revolutionary or a Conservative Approach – Law of Probate and Law of Responsibility

To the question, must we profoundly modify the legislation bearing on probate law to take into account the reality of computers and communications technology? The reader may press the question, yet the reply, in my opinion, must be for the most part negative. It is not for us to revolutionize a law whose concepts not only embrace the new reality but even impose upon it the need to respond to qualities and demands derived from its own concepts. Doubtless, we are going to envisage certain additions, even establish the accompanying mode necessary to guarantee this response! This will be the object of point 2.2.

Beyond that which can well be called a quiet revolution, recent regulations on the electronic transfer of funds lead us to a still more essential reflection, that of installing rules of responsibility for those who place facilities for the conclusion of transactions at the disposal of others. The law of responsibility mitigates the consequences of certain gaps in the traditional law of probate

and entails repercussions for the same. Whether it is a matter of one law or another, the purpose is still, as always, that of protecting the expression of free will (Section 2)

2.2. Regulation of Probate Law

2.2.1. Rejection of All Revolution

Negatively, section 1 demonstrates the suitability of electronic documents to the traditional concepts of probate law. In other words, there is absolutely no need for legislation in the form of new concepts, but rather for deepening the traditional provisions with regard to their finalities.

Positively, it proclaims the equivalence of principle which excludes any a priori rejection by the judge of an electronic document.

1) It seems to us therefore, that with regard to the latter, that the position of the Council of Europe[15] is by no means justifiable in recommending, as a step toward electronic proof, the suppression in all member countries of the requirement to furnish an instrument. On the contrary, the tendancy of our argument is to show the use of an adherence to traditional concepts in probate law: this use leads one to place certain demands or 'criteria' of acceptability upon electronic documents functioning as signed documents or faithful copy within the meaning of the law.

2) We equally target the Luxembourgeois and French reforms. Both of these aim essentially at delineating the types of impossibility to which article 1348 of the Belgian civil code refers. To recap, article 1348 is intended to liberate the judge from the constraint constituted by article 1341 of the civil code in cases *where it has been impossible for the parties to draw up an instrument.* As is still the case in Belgium, the original text of article 1348 of the civil code did not specify whether the impossibility of producing written proof of an obligation was material or moral. That has been dealt with since and the operative distinction dissipates any doubt on that heading. The absence of written proof arising from the use of new methods of data transfer may constitute a material impossibility and therefore falls under the provisions of article 1348.

This reform of article 1348 seems to us regrettable for various reasons. Firstly, it is unfortunate that the adaption of probate law to the new technology should take the form of this exception dispensing with the need for written proof. It may now be feared that the extension thus given to article 1348 may cause article 1341 of the civil code to be emptied of all content and that the rule of liberty in matters of probate may thus be installed, much as we have experienced it in commercial matters.

Furthermore, it seems to us to be unacceptable to say that the use of new technologies involves the absence of written proof. Whenever data is exchanged, even computer data, an instrument either exists, or at the least there is the possibility of drawing one up, not an instrument taken in the restrictive sense of the term, but certainly an instrument in an evolutionary perspective.

Finally, there is a logical contradiction in admitting that the use of computers constitutes a case where the procurement of an instrument is impossible. In reality, the impossibility does not exist, it is more a matter of the parties, usually one of them,[16] namely the one who foresees the use of electronic proof, have decided to have absolutely no recourse to paper.

2.2.2. Taking the Traditional Regulations Seriously[17]

The equivalence of principle we affirmed above leads to a strict application of legislation on probate. Some consequences can be deduced from this within the framework of our legislation. If, for example, we can admit that a duly authenticated electronic document is, in certain cases, an instrument of simple private contract generated by the person against whom it is being opposed, such an instrument, to the degree in which it fails to fulfil the formality of a double, will not enjoy the full probative value of article 1325 of the civil code, but rather that of an initial essay at written proof in the sense of article 1347 of the Belgian civil code. We may not forget that the signature, whether manuscript or on paper can be the object of a motion of disavowal ... the motion will bear upon the falsification of the means of identification, or its usurpation by a third party.[18]

Finally, numerous specific dispositions which impose a written instrument in certain contracts, such as contracts of credit or insurance, should be able to be concluded electronically, except in such cases where the formality is imposed ad solemnitatem.

In our opinion, beyond this simple application of traditional regulations, legislation is called for in the matter of 'faithful copy', which in our code would be inserted into article 1334 of the civil code which deals with copy. We would propose the following text: 'A document reproduced from a recording of a signed instrument onto an information support is considered as a copy'.

'The above rule is excepted when one of the parties or their authorized agent has not conserved the original and produces copies made from these originals under the responsibility of the person in whose keeping they are. These may have the same value in probate as the signed instruments of which they are presumed, unless proved to the contrary, to be faithful copies, since the originals were recorded according to the security criteria established by the King'.

2.2.3. A Call for Normalization

Any consideration of a document as equivalent is conditional on its subordination to proof that the electronic processes of conclusion and conservation meet the requirements set out above. The content of these requirements should develop according to technological evolution and the parameters arising from each concept. There is no question of defining once and for all the concrete implications of each parameter on the basis of the current state of technology. The reliability and durability of a signature supposes, therefore, the use of ever more advanced and more secure cryptographic methods.

As is easy to concieve, the difficulty for a company or administration which wishes to avail itself of electronic proof resides in the quality of the security measures required. In this area, a movement in favour of normalization will naturally emerge within the institutions concerned which, without being obligatory, will nonetheless represent an acceptable standard for the courts, with the reservation of expert authentification should they deem it necessary. The advantage of such normalization is its relative flexibility. One would in the meantime remain alert to the possibility of consumer representatives participating in the process of normalization.

This tendancy toward normalization, by definition a priori of quality standards relating to programs and methods which oversee the drawing-up and conservation of contracts, enables us to introduce that which we think of as the merging of probate law into law of responsibility. The debate on proof comes down often to the need to determine whether the person wishing to take advantage of electronic proof has fulfilled all the conditions laid down, in default of which he will be judged as not having taken the necessary precautions and therefore held responsible, inasmuch as he is unable to produce adequate proofs.

Our intention here is to show that, as a result of recent regulations on the electronic transfer of funds, the question of responsability may, at the limit, replace that of proof.

2.2.4. From Proof to Responsibility: The Case of Electronic Transfer of Funds

We do not wish to deal here with the question of the responsibility of a banker in the matter of electronic payment services,[19] but rather to draw, from recent regulations or jurisprudence on the subject, some new ideas on the responsibility of someone who offers electronic transaction services. Beyond this, we intend to underline the links between these new obligations and probate law.

Without being exhaustive, some ideas can be picked out:

- a banker's obligation to inform the user of electronic modes of payment of the risks that can be incurred with an electronic signature and to insist on the need for guarding and maintaining the confidentiality of his access code. This obligation has been recognized notably by the European Council's recommendation of the 17 November 1988;
- a banker's obligation, as soon as there has been a banker's obligation, as soon as there has been *a disavowal of a signature*, to engage a system of opposition with immediate effect;[20]
- finally and most important, in the event of the electronic trace of a banking operation being contested, the banker's obligation under the European recommendation[21] to prove 'that the operation was correctly carried out and was not affected by a technical malfunction or any other deficiency of the system'. This obligation placed at the feet of the banker to prove the reliability of his recording and demonstrate the security of his information system[22] is enunciated even more precisely by article 4.A. of the American payment act, which calls for a banker to set-up reasonable security procedures before permitting the verification of the origin of messages or detecting errors affecting them.[23]

This last obligation is considered as 'essential'. In other words, even if contractual liberty frees the banker from the traditional burden of proof, he cannot avoid having to demonstrate in advance the quality of his provisions for the drawing-up and conservation of electronic proof. To put it differently, the emergence of this new responsibility places on the banker an obligation of 'prima facie proof', according to the expression that has become well-known since the American E.F.T. Act.[24]

Thus, without having to touch traditional probate law, jurisprudence, doctrine and already even regulative changes charge a person who places electronic transaction services at the disposal of the public and takes advantage of electronic proof, with an obligation from which he may not depart: that of proving the security of his system. In other words, the law of responsibility here takes up the baton from traditional probate law.

Conclusions

The reader who has decided to follow us this far, will draw with us the consequences of an approach designed to 'closely adhere to the law of probate, its principles and its finalities'.[25] For my part, and without pretending to be exhaustive, I can think of six:

- The approach takes into account the fundamental inbalance that exists between the two parties to an electronic transaction, due to the fact that

only one of them organizes and controls access, storage and the processes necessary for the drawing-up and conservation of the parties. It is therefore of primary importance that the person who can take advantage of an electronic document to furnish proof of a transaction, must be held responsible for proving the security of the system, that is to say, its reliabiity, integrity and availability.

- The owner of the system's obligation to comprehensively inform the user of the consequences of that use and of the risks such use might incur, is added to the obligation to provide proof of the system's quality in the case of relations between businesses and consumers. Parallel to the owner's responsibility to inform the user is the latter's obligation to inform him- or herself of the consequences of participation in the system.
- Once the person responsible for the system has discharged these obligations, the judge, who will have availed himself of the opinion of experts, should be led, depending on the case, to regard documents produced by new information and communication technologies as signed instruments and to accord them the force in probate which the law assigns to such signed instruments, neither less nor more.
- This done, the proposed approach does not seek to introduce any probate regulations specific to computers. It simply presumes that the notions of instrument and signature should be defined in a manner independant from any material support and only with reference to their inherent parameters and purpose.
- The approach by general legal prescriptions to a preference for a specific technological law should enable us to avoid any rigid restriction on the receivability of electronic documents to a temporary technical state-of-the-art.
- In that which concerns archives, reliance on electronic support media obliges that operation be demonstrated as being in conformity with the demands of fidelity, durability and inalterability. This is a heavy responsibility and a proof difficult to carry, particularly when taking into account the dangers of fraud and of attempts on the integrity of documents while within an archive, or during a transfer from one support to another, etc. Here equally, regulatory norms made while carrying out the law enable the latter to guard its general character, while allowing the commercial sector to benefit from norms of judicial security necessary to their transactions.

What can we add to this?

The debate: 'Probate law and new information and communication technologies' has hardly started: yesterday mere isolated phenomena, computer

transactions will become the quotidian standard of tomorrow, whether in relations between professionals, in contracts between private citizens, in dealings between the latter and professionals or between both of these and their governments. Tomorrow we shall file our tax returns, reserve a table or book a flight, all by computer.

The solution to the debate can only reside in the sanction of technology, which recalls each to accept *responsibilities*:

- the users of a service, that of being conscious of the extent of their commitment and the need to respect such reasonable security norms as are explained to them (e.g., informing without delay in the event of losing a credit card);
- companies, that of informing their customers of the risks entailed in the use of such systems and of offering systems of quality as regards production and conservation of electronic documents;
- government or other authorities, that of defining, both among themselves and in their relations with business and private citizens, new modes of dialogue;
- institutions responsible for setting-up norms, that of proposing security standards of both a general and specific nature for particular sectors, taking into account the interests of all parties;
- judges, that of forging their own personal convictions, with the aid of experts.

Notes

1. Paper presented to the colloquium on 'Data processing and law' held in Montreal from the 30 September to the 3 October 1992 and organized by the Quebec Association for the development of juridic data processing (AQDIJ).
2. The aim of these reflections is not to give an analysis of the state of various legislations in force in continental law, but to distill certain constants from their practice and evolution. Such an analysis is proposed by numerous publications, to whose pages we would direct the reader, such as:
   - M. Antoine, M. Eloy, J.F. Brakeland (1991) Le droit de la preuve face aux nouvelles technologies de l'information, *Cahiers du CRID* 7, Bruxelles, Story-Scientia.
   - I. de Lamberterie (éd) (1990), La valeur probatoire des documents informatiques, Probat, Rapport établi pour la Commission européenne (non-published, hereafter referred to as the 'Probat-study').
   - X. Linant de Bellefonds, *Informatique et droit de la preuve*, Travaux de l'AFDI, Paris, Ed. des Parques, *The legal position of the Member States with respect to Electronic Data Interchange*, Report achieved on behalf of the European Commission by the Law Office of Lodomez-Crouquet, 1989.
   - F. Gallouedec-Genuys (1990) *Une société sans papier, nouvelles technologies de l'information et droit de la preuve*, Paris, La documentation française.

- J. Larrieu (1988) *Les nouveaux moyens de preuve: pour ou contre l'identification des documents électroniques à des écrits sous seing privé*, Lamy Droit de l'Informatique, H.
- M.S. Baum and H.H. Perrit jr. (1991) *Electronic Contracting, Publishing and EDI Law*, Willey Law, New York 1991, 66.23–29 (evidentiary issues).
- B. Wright (1991) *The Law of Electronic Commerce*, Little, Brown and Company, Boston, pp. 95–164 (legal proof issues).
- S. Castell (1991) Evidence, authorisation and security – is EDI legally reliable?, *The Computer Law and Security Report* 6(5): 2–8.
- T. Dosdale (1991) Can EDI be trusted – Endangered Data Interchange, *The Computer Fraud and Security Bulletin*: 14–17 (January).
- UNCITRAL (1985) Report of the Secretary-General, Legal Value of Computer Records, A/CN.9/265, February 21.

3. 'In principle, rules on the preeminence of written proof are of no interest to law and order. The parties concerned may renounce the right of recourse to them, in this regard they are free to make whatever agreements they chose' (P. Van Ommeslaghe (1975) Les obligations, *RCJB* 122: 170). The principle of contractual liberty in that which pertains to proof and the non-constraining character of legal measures taken in this respect, seem to be accepted by the majority of European countries (in this regard, M. Antoine *et al.*: 50 et seq.).
4. The PROBAT study carried out by the European Commission asserts that these three concepts are recognized as fundamental in all European judicial systems, although certain countries (those depending on 'legal' proof) may accord them a probative and constraining value superior to others.
5. Our reflections relative to the equivalence of the electronic signature and the written signature on the one hand, and the equivalence of electronic and written documents on the other, are based largely on those of M. Antoine and M. Eloy, op. cit.: 64 to 67 in particular. We also direct the reader to: Commission of the European Communities, Electronic Signature, The key to mobility, Workshop Report, Brussels, December 1992; C. Reed (1989) Authenticating Electronic Mail messages – Some evidential problems, *Modern Law Review* 52: 649–660; B. Amory and Y. Poullet (1987) Computers in the law of evidence – a comparative approach in civil and common law systems, *Computer Law and Practice*: 114–124; R. Bradgate, Evidential issues of EDI, in I. Walden (1989) *EDI and the Law*, London, Blenheim Online Publications, pp. 9–42.
6. Cf. the table prepared by Mssrs. Antoine and Eloy in M. Antoine *et al.*, op. cit.: 63.
7. Trusted third parties and similar services, Report achieved on behalf of the European Commission by the Law Office of Barents, Gasille and Mout, Brussels, November 1991; M. Baum, The electronic notary, in M. Baum, Electronic contracting, publishing, and EDI Law, by Wiley Law Publications, New-York, 1991.
8. Z.P.O. § 415 F.
9. By 'directly readable', one understands that the system should be capable of reproducing the information almost instantly in an immediately readable form.
10. In particular, the already vintage French jurisprudence on article 1347 of the Napoleonic code which, with regard to the opening procedure for proof by writing, admits sound recordings and photography etc. Cf. in the same respect, the Dutch, Luxembourgois, Portugese and Irish doctrines and jurisprudence (cf. TEDIS, op. cit., and I. de Lamberterie (ed.), report cited, p. 57).
11. Fiscal instruction dated 27 December 1991, taken in application of article 47 of the amended law of finances (ar. 47 de la loi des finances rectificative pour 1990, n° 90–1169, du 29 décembre 1990, JO 29 décembre 1990). On this matter, see Th. Piette-Coudol (1991), *L'EDI et le droit*, Ed. Hermès, Paris.
12. In this respect, I de Lamberterie writing in *La valeur probatoire des documents informatiques dans les pays de la CEE*, RIDC, 1992, p. 662:

" 'Inalterable', 'durable', what do these terms mean? One can find no definition in jurisprudence and the definitions otherwise given are not equivalent: for some 'inalterable' means that one may not modify the document, for others it means that the document has not been modified."

13. Similarly in Spain, Greece and Portugal where copies must be authenticated, or in The Netherlands and Belgium where they must be certified.
14. This is the qualifier employed by the French (art. 1348 C.C.) and Luxembourgeois legislations (art. 1348 C.C.) in response to the concern referred to here.
15. Recommendation R(81) 20 relative to the harmonizing of legislations in the matter of requiring a written instrument and in that which pertains to the inadmissability of reproductions of documents and of computer recordings. The first recommendation concerns the suppression, in a maximum of cases, of the use of a written instrument as a means of proof ...
16. The bank, in that which pertains to the electronic transfer of funds.
17. Cf. on this point, the text produced by the Centre de Recherche Informatique et Droit of the FUNDP in Namur, on the demand of the Justice Minister and the dossier M. Antoine and J-F. Brakeland (1992) Le Droit de la preuve face aux nouvelles technologies de l'information, Dossier, *Nouvelles des Technologies de l'information* 54, Brussels, 09/06/1992.
18. The recognition of an electronic signature as a signature should permit the application of other dispositions relative to signatures. In Belgian law it is used to underscore the fact that, in virtue of article 1323 of the civil code, the person against whom one opposes a simple private contract, is obliged to formally recognize or disavow his or her signature (or handwriting). In the event of a disavowal, judicial verification is required (article 1324 of the civil code), in conformity with article 883 et seq. of the judiciary code.
19. On this point, refer to E. Meysmans and X. Thunis (1992) The regulating of credit cards in Belgian and European law, in *La nouvelle loi sur le crédit à la consommation*, Brussels, CREADIF, 128 et seq.
20. Cf. article 8.2 of the recommendation.
21. Cf. article 6.2 of the recommendation.
22. Cf. also the recommendation of the U.K.'s recent Jack Report.
23. The reference to 'reasonable security' supposes an evolutionary development. We also note the obvious reference to normalization (cf. already *supra* n° 20).
24. On the E.F.T. Act, see X. Thunis and M. Schauss, Aspects juridiques de paiement par cartes, *Cahiers du C.R.I.D.* 1, Brussels, Story-Scientia, p. 35 et seq.
25. This is the wish of Ms. Gallouedec-Genuys, op. cit.: 59.