LITIGATION IN E-COMMERCE: PROVING A CASE WITH ELECTRONIC DOCUMENTS

FRANCISCO ED. LIM*

I. THE CONCEPT OF DOCUMENTS AS EVIDENCE

The concept of documents as evidence, as stated in the Rules of Court, "consist of writings or any material containing letters, words, numbers, figures, symbols or other modes of written expression offered as proof of their contents."[1]

When a party tenders a document as evidence, certain issues determine the admissibility of the document.

First the question on authentication - what is the document? Is the document what it purports to be? Second, the inquiry into the Best Evidence Rule - is the document offered to prove its contents? If so, is it the original? If not the original, is it a copy that is admissible under any of the exceptions to the Best Evidence Rule? Finally, the question regarding hearsay - is the document offered for the truth of the assertions that it contains? If so, is it admissible under an exception to the Hearsay Rule? These three basic questions are equally applied to electronic documents presented as evidence.

II. THE STATUS OF ELECTRONIC DOCUMENTS BEFORE THE E-COMMERCE ACT

Prior to the enactment of the E-Commerce Act (ECA), the Supreme Court decided two cases which embodied the Court's attitude regarding electronic documents as evidence. The first of these cases, decided in 1991, is *People v. Burgos.*[2]

Burgos was prosecuted for a violation of R.A. 1700, otherwise known as the Anti-Subversion Act. During the bail hearing, the prosecution sought to present a witness who would print, as evidence before the court, data contained in computer diskettes seized from the accused by virtue of a

---

Cite as 45 ATENEO L. J. 355 (2001)

* LL.B. 1981, Ateneo de Manila University School of Law; LL.M., University of Pennsylvania; Editor in Chief (1979-1981), *Ateneo Law Journal.*

1 1997 Revised Rules of Court, Rule 130 (1997).

2 200 SCRA 67 (1991).

search warrant. The trial court disallowed the printing of the contents of the diskettes because (a) the diskettes were in the possession of the prosecution; and (b) they could be manipulated, as admitted by the witness himself.

The Supreme Court held that the trial court should have allowed the documents to be printed before it, as follows:

> We therefore hold that the printing out of data (if any) encoded in the diskettes should be allowed. Respondent Judge's asserted apprehension that the witness brought by the prosecution to undertake the printing out of the diskettes' contents could himself "manipulate" said diskettes during the actual printing out in court may very easily be relieved by designating a competent person agreeable to both parties, and especially to the respondent Judge, who can perform the task of printing out the contents of the diskettes. Respondent Judge's ostensible lack of confidence in the prosecution witness should not in any way affect the integrity of the diskettes themselves or the right of the prosecution to show the contents of the diskettes subject, of course, to the applicable rights of the accused.

The second case on electronic documents decided by the Supreme Court was the 1999 case of *IBM Philippines, Inc. v. Pena*.[3] In that case, IBM Philippines, Inc. (IBM) terminated an employee, Angel Israel, on the ground of habitual tardiness and absenteeism. Israel asserted that he was illegally dismissed and was denied due process. IBM contended that, on the contrary, the employee's supervisor sent him numerous e-mail messages regarding his tardiness and absenteeism, which constituted sufficient notice of the charges against him. In their position paper, IBM attached copies of these printed e-mail messages, which they sought to admit as evidence.

In ruling that the computer print-outs were inadmissible, the Supreme Court declared that while administrative agencies are not bound by technical rules of procedure, the basic evidentiary rule remains: the evidence presented must at least have a modicum of admissibility to be given some probative value.

In particular, the Court ruled that the computer print-outs were inadmissible for lack of proper authentication as follows:

> "[t]he computer print-outs, which constitute the only evidence of petitioners, afford no assurance of their authenticity because they are unsigned."

[3] 305 SCRA 592 (1999).

> Not one of the computer print-out copies submitted by petitioners was ever signed, either by the sender or the receiver. There was thus no guarantee that the message sent was the same message received. As the Solicitor General pointed out, the messages were transmitted to and received not by the private respondent himself, but by his computer. **Neither were the computer print-outs certified or authenticated by any company official who could properly attest that these came from IBM's computer system or that the data stored in the system were not and/or could not have been tampered with before the same were printed out.** It is noteworthy that the computer unit and system in which the contents of the print-outs were stored were in the exclusive possession and control of petitioners since after private respondent was served his termination letter, he had no more access to his computer.

Burgos and *IBM* highlighted two evidentiary problems related to computed-based documents courts then faced, namely, the integrity and authenticity of the electronic documents.

III. THE E-COMMERCE ACT

The E-Commerce Act[4] defines electronic data message and electronic document as follows:

> SEC 5. Definition of Terms –
>
> xxx
>
> (C) "Electronic data message" refers to information generated, sent, received or stored by electronic, optical and similar means.
>
> xxx
>
> "(f) "Electronic document" refers to any representation of information, data, figures, symbols or other modes of written expression received, recorded, transmitted, stored, presented, processed, retrieved or produced electronically.

[4] An Act Providing for the Recognition and Use of Electronic Commercial and Non-commercial Transactions and Documents, Penalties for Unlawful Use Thereof and for Other Purposes, R.A. 8792, § 7 (2000) [hereinafter ECA].

The Implementing Rules and Regulations of the ECA (IRR) further state:

> Section 6. Definition of Terms.
>
> xxx
>
> (h) "xxx Throughout these Rules, the term "electronic document" shall be equivalent to and be used interchangeably with "electronic data message."

IV. SALIENT FEATURES OF THE E-COMMERCE ACT RELATING TO THE RULES ON EVIDENCE

A. FUNCTIONAL EQUIVALENT RULE

The ECA adopts the "functional equivalent approach" in treating electronic documents. Under the ECA, for evidentiary purposes, an electronic document is the functional equivalent of a paper-based document, and an electronic signature is the functional equivalent of a traditional signature.[5]

Thus, take a case where X Co., Inc., an investor lending company, loaned P1,000,000 to Y, and for one reason or another, no promissory note was executed by Y in favor of X Co. The loan is, however, evidenced by two (2) e-mails – one from X Co. saying that Y can pick up the check from the X Co.'s main office, and the other is an e-mail from Y asking for 30 days extension to pay the loan. Thereafter Y failed to pay the amount after the extended due date. X Co. then files a collection suit against Y. As part of its evidence to prove the loan, X Co. presents the two (2) e-mails as evidence.

Since under the ECA, the e-mails are the **functional equivalent** of the traditional paper-based documents, Y cannot validly object to the admission of the e-mails on the sole ground that they are not in the form of traditional paper-based documents.

Using the same example above, assuming that X Co. records all its loan receivables from customers in its computer system, X Co. may then present a computer print-out showing that Y has a loan payable to the company to further prove its case. This is because the computer print-out is the **functional equivalent** of the traditional paper-based document.

B. NON-DISCRIMINATION RULE

The ECA is basically a rule of non-discrimination against electronic

[5] ECA, § 7.

documents. By itself, it does **not** make an electronic document legally effective, valid and enforceable. What the ECA merely does is **to not discriminate against** electronic documents, i.e. "**there should be no disparity of treatment between data messages and paper documents**" as evidence.[6] Accordingly, the ECA is **negatively** phrased as follows:

> Section 6. *Legal Recognition of Electronic Data Message.* – Information shall not be denied validity or enforceability solely on the ground that it is in the form of electronic data message purporting to give rise to such legal effect, or that it is merely incorporated by reference in that electronic data message.

Based on the above, the ECA does not state that the electronic data message is valid and enforceable. By stating that the "[i]nformation shall not be denied validity or enforceability **solely** on the ground that it is in the form of electronic data message", Section 6 "merely indicates that the form in which certain information is presented or retained cannot be used as the **only** reason for which the information would be denied legal effectiveness, validity or enforceability."[7] Article 6 "**should not be misinterpreted as establishing the legal validity of any given data message or any information contained therein.**"

The ECA adopts this principle of **non-discrimination** insofar as the rules on evidence are concerned.

> Section 12. *Admissibility and Evidential Weight of Electronic Data Messages or Electronic Documents* – In any legal proceedings, *nothing* in the application of the rules on evidence shall *deny* the admissibility of an electronic data message or electronic document in evidence –
>
> On the sole ground that it is in electronic form; or
>
> On the ground that it is *not* the standard form xxx (undersocring supplied).

C. ECA NOT A RULE ON AUTOMATIC ADMISSIBILITY

The ECA does not automatically make electronic documents admissible in evidence. The electronic document must still meet the

[6] *See* UNCITRAL Model Law on Electronic Commerce (1996) with additional article 5 as adopted in 1998 and Guide to Enactment [hereinafter UNCITRAL Enactment Guide].

[7] *Id.*

requirements for admissibility prescribed by our rules on evidence. Thus, the ECA is once again **negatively** phrased as follows:

Section 12. *Admissibility and Evidential Weight of Electronic Data Messages or Electronic Documents* – In any legal proceedings, nothing in the application of the rules on evidence shall *deny* the admissibility of an electronic data message or electronic document in evidence.

Rather than saying an electronic data message or electronic document *shall be* admissible in evidence, Section 7 of the ECA expressly provides that it "**does not modify** any statutory rule relating to the admissibility of electronic data messages or electronic documents, except the rules relating to authentication and best evidence."

V. REQUISITES FOR THE ADMISSIBILITY OF ELECTRONIC DOCUMENTS

Like any other type of documentary evidence, an electronic document or computer-generated document must still comply with the following requisites for admissibility:

A. RELEVANCE

The electronic document sought to be admitted into evidence must have a relation to the fact in issue as to induce a belief as to its existence or non-existence.[8] This requirement was affirmed in the *IBM* case, where the e-mails were relevant evidence, because they tended to prove the main issue in the case - the legality of the employee's dismissal.

B. COMPETENCE

The electronic document must not be excluded by the law or rules on evidence.[9] In other words, evidence is competent when it is not excluded by law in a particular case.

The Constitution establishes exclusionary rules that render certain types of evidence inadmissible. Notably, evidence obtained in violation of the right against unreasonable searches and seizures or the privacy of communication and correspondence,[10] confessions and admissions taken

[8] 1997 Revised Rules of Court, Rule 128, § 4.

[9] 1997 Revised Rules of Court, Rule 128, § 3.

[10] 1987 PHIL. CONST. art. III, §§ 2 & 3.

in violation of the rights of a person during custodial investigation,[11] and in violation of the right against self-incrimination.[12] Moreover, Wiretapping and other related violations of the privacy of communications are prohibited and penalized by the Anti-Wiretapping Act.[13] The Rules of Court likewise exclude certain types of evidence, for instance, evidence in violation of the best evidence rule, the parol evidence rule, the disqualification by reason of marriage, or privileged communication.

Assume that there is a collection case filed by A against B. A knows that C, wife of B, e-mailed her husband, urging him to pay A, using their Citibank money market placement to effect payment. B replies by e-mail saying that while they have the money to pay A, he does not want to do so because he feels that A cheated him in another transaction. In such a case, A cannot subpoena the e-mails to prove that B owes him the money, or that B's failure to pay is attended by bad faith. The communication between spouses B and C, though in electronic form, remains privileged under the marital communications rule.[14] The ECA does not modify this marital privilege.[15]

In *Burgos*, had the diskettes been seized without a search warrant, and had the trial court allowed the contents of the computer diskettes to be printed, the evidence would have remained inadmissible for the diskettes were illegally obtained.[16] The ECA did not modify this exclusionary rule of the Constitution.[17]

C. AUTHENTICATION

Finally, the electronic document must be what it purports to be.[18]

Supposing X owed Y a sum of money, and Y wishes to present e-mail from X asking for an extension of time to pay the loan. Before the e-mail can be admitted into evidence, Y must first present evidence that it is the very same e-mail sent by X. In the words of the ECA, the "electronic data message or electronic document is what the person claims it to be."[19] Otherwise, as

[11] 1987 PHIL. CONST. art. III, § 12.

[12] 1987 PHIL. CONST. art. III, § 17.

[13] Anti-Wiretapping Act, R.A. 4200.

[14] 1997 Revised Rules of Court, Rule 130, § 24(a).

[15] ECA, § 7.

[16] 1987 PHIL. CONST., art. III, § 2 & 3.

[17] ECA, § 7.

[18] 1997 Revised Rules of Court, Rule 132 § 20.

[19] ECA, § 11[b].

in the *IBM* case, the court cannot receive it in evidence for lack of proper authentication.[20]

VI. THE ECA AND THE BEST EVIDENCE RULE (ORIGINAL DOCUMENT RULE)

The Best Evidence Rule is contained in Rule 128 of the Revised Rules of Court:

> SEC. 3. ***Original document must be produced; exceptions.*** – When the subject of inquiry is the contents of a document, no evidence shall be admissible other than the original document itself, except in the following cases:
>
> (a) When the original has been lost or destroyed, or cannot be produced in court, without bad faith on the part of the offeror;
> (b) When the original is in the custody or under the control of the party against whom the evidence is offered, and the latter fails to produce it after reasonable notice;
> (c) When the original consists of numerous accounts or other documents which cannot be examined in court without great loss of time and the fact sought to be established from them is only the general result of the whole; and
> (d) When the original is a public record in the custody of a public officer or is recorded in a public office.

Simply stated, the Best Evidence Rule (BER) provides that no evidence other than the original is admissible **to prove the contents of the writing**. This is to avoid the possibility of misinterpreting the contents of the document.

The BER applies equally to electronic documents. For instance, consider a collection case between X and Y, where X claims, as a defense, that what he owes Y is P100,000 and not P1,000,000. Should X assert that B sent him an e-mail acknowledging the debt to be P100,000, X would not be able to present a photocopy of the e-mail; he must present the e-mail itself because what is at issue is the contents of the e-mail.

In the *IBM* case, suppose the employee claimed that IBM's e-mails failed to warn him, but rather, condoned his absences and tardiness; IBM should present the computer print-outs themselves and not any other evidence, unless excused under the BER.

[20] 1997 Revised Rules of Court, Rule 132, § 20.

A. Compliance with the Best Evidence Rule under the ECA.

The BER requires that the original of the document be presented when its contents are in issue. However, what is the original of the electronic document? Is it the data contained in the diskette or the diskette itself? Can a print-out be considered as the original?

In the United States, the Federal Rules of Evidence provide:

> Rule 1001. **Definitions**
>
> For purposes of this article the following definitions are applicable:
>
> xxx
>
> (3) Original. xxx If data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an "original." xxx
>
> Rule 1002. Requirement of Original
>
> To prove the content of a writing, recording, or photograph, the original writing, recording, or photograph is required, except as otherwise provided in these rules or by Act of Congress.

Thus, a print-out, if shown to reflect the computer's data accurately, is an "original" of the computer-stored data so that the diskette need not be introduced in evidence.

The ECA provides that where the law requires information to be presented or retained in its original form, that requirement is met by an electronic document if:

> 1. The integrity of the information, from the time it was first generated in its final form, is shown by evidence *aliunde*; **and**
>
> 2. Where the information is required to be presented, that the information is capable of being displayed to the person to whom it is presented.[21]

In other words, an electronic document is considered an original

[21] ECA, § 10[1].

document for purposes of the BER. Note that unlike the traditional BER under the Rules of Court, the ECA prescribes two (2) requirements before an electronic document can be considered the functional equivalent of an original document, namely:

1. **Integrity** which must be established by evidence *aliunde* or otherwise; and

2. **"Display-ability"** - that the information is capable of being displayed to the person to whom it is to be presented.

B. Elements of proof to establish the Integrity of an Electronic Document

Before an electronic document may be considered as the functional equivalent of an original document under the ECA, its integrity must first be proved. This may be done by:

1. Extrinsic evidence (*i.e.*, evidence other than the electronic document) that the electronic document has remained complete and unaltered apart from the addition of any endorsement and any change which arises in the normal course of communication, storage and display; and

2. (a) The information or communication system was operating in a manner that did not affect the integrity of the electronic document or electronic data message and there are no reasonable grounds to doubt the integrity of the information and communication system; or

   (b) The electronic data message or electronic document was recorded or stored by a party to the proceedings adverse in interest to the party using it; or

   (c) The electronic data message or electronic document was recorded or stored by a person who is not a party to the proceedings, and who did not act under the control of the party using the record. [22]

Note also that the UNCITRAL Enactment Guide states that the integrity of the electronic information is assessed by "reference to systematic recording of the information, assurance that the information was recorded without lacunae and protection of the data against alteration."[23]

[22] ECA, § 11.

[23] *See* UNCITRAL Enactment Guide, *supra* note 6.

VI. AUTHENTICATION OF ELECTRONIC DOCUMENTS

A. BURDEN OF PROOF

Section 11 of the ECA provides that "the person seeking to introduce an electronic data message or electronic document in any legal proceeding has the burden of proving its authenticity by evidence capable of supporting a finding that the electronic data message or electronic document *is what the person claims it to be.*" (emphasis supplied)

B. ELEMENTS OF PROOF IN AUTHENTICATING AN ELECTRONIC DOCUMENT

The authentication of electronic data or of an electronic document can be done by demonstrating, substantiating, and validating a claimed identity of a user, device, or another entity in an information or communication system by proof that an appropriate security procedure, when applicable, was adopted and employed for the purpose of:

a) verifying the originator of an electronic data message or electronic document; or

b) detecting error or alteration in the communication, content or storage of an electronic document which, using algorithm and codes, answers back or acknowledgment procedures or similar security devices.

An example of the second way is encryption authentication. Through this process, a public key encryption which uses a combination of private and public passwords is used to ensure the confidentiality and authenticity of the message, *i.e.,* that it was actually created by the purported author and that it has not been altered. A sender can place an electronic "signature" on a message to ensure its authenticity by encrypting the message with the sender's private password. The recipient then uses the sender's public password to decode the message. The sender's public password will only decode the message if the message was encrypted with the sender's private password; and the message was not modified or altered in any way during the transit.

C. OTHER MEANS OF AUTHENTICATION

The ECA expressly provides that an electronic document or signature may be authenticated by **"other ways,"** *i. e.*, means other than what is enumerated by Section 11 of the Act. Hence, authentication may be done by:

1. Testimonial Sponsorship

A witness may be called by the party presenting the electronic document to testify that the electronic document is what the proponent claims it to be. For instance, in a collection case filed by A against B where A presents an e-mail sent by B, testimonial sponsorship would operate if A presents B's secretary who testifies that the e-mail presented is the same e-mail sent by B to A.

In the *IBM* case, the Supreme Court found the computer print-outs should have been certified or authenticated by a company official. Such official could have attested that they came from IBM's computer system or that the data stored in the system was not or could not have been tampered with before they were printed out. On the other hand, in *Burgos*, the print-outs, if allowed by the court to have been made, could have been authenticated by testimony that: (a) the diskette was the same diskette seized from the accused; (b) that the contents of the diskette were not tampered with; and (c) that the print-out accurately reflects the contents of the diskette.

2. Circumstantial Evidence

Circumstantial evidence may be used when the person presenting the electronic document can demonstrate that the electronic document contains information only the creator would know, or that the disputed document was replied to.

In the *IBM* case, the employee denied having received any of the e-mails sent to him regarding his tardiness and absenteeism. If there were reply e-mails from the employee, IBM could have produced them in evidence and the same could have "authenticated" IBM's e-mails to him.

3. Authentication via an intermediary

The parties may agree to send each of their electronic messages through a trusted intermediary who retains a copy of each transmission. If a question arises as to the contents or originator of a particular communication, the intermediary can easily resolve the dispute by consulting its copy of the message.

4. Any other method mutually agreed upon by the parties.

The parties may stipulate as to the authenticity of an electronic data message or document instead of presenting evidence thereon. Pertinently, the ECA provides:

> SEC. 38. *Variation by Agreement.* As between the parties involved in generating, sending, receiving, storing or otherwise processing electronic data message or electronic document, any provision of this Act may be varied by agreement between and among them.

VII. ELECTRONIC SIGNATURES

An electronic signature is "any distinctive mark, characteristic and/or sound in electronic form, representing the identity of a person and attached to or logically associated with the electronic data message or electronic document or any methodology or procedures employed or adopted by a person and executed or adopted by such person with the intention of authenticating or approving an electronic data message or electronic document."[24]

An electronic signature need not be the traditional signature of a person in digital form.

A. REQUIREMENTS FOR ELECTRONIC SIGNATURE TO BE THE FUNCTIONAL EQUIVALENT OF TRADITIONAL SIGNATURE

To be considered the functional equivalent of a traditional signature, an electronic signature must be proved by showing that a prescribed procedure, not alterable by the parties interested in the electronic document, existed under which:

1. The method is used to identify the party sought to be bound and to indicate said party's access to the electronic document necessary for his consent or approval through electronic signature;

2. The method is reliable and appropriate for the purpose for which the electronic document was generated or communicated, in the light of all circumstances, including any relevant agreement;

3. The party sought to be bound, in order to proceed further with the transaction, to have executed or provided the electronic signature; and

4. The other party is authorized and enabled to verify the electronic signature and to make the decision to proceed with the transaction authenticated by the same.[25]

---

[24] ECA, § 5

[25] ECA, § 9.

B. PRESUMPTIONS REGARDING ELECTRONIC SIGNATURE

1. It belongs to the person to whom it correlates;

2. It is affixed with the intention of signing or approving the electronic document, unless:

a) The person relying on the electronically signed document knows or has notice of defects in or unreliability of the signature; or

b) Reliance on the signature is not reasonable under the circumstances.[26]

The presumption of the integrity of an electronic signature established above "may be presumed to have been established by an affidavit given to the best of deponent's knowledge," subject to the right of adverse party to cross-examine the deponent.[27]

C. AUTHENTICATING AN ELECTRONIC SIGNATURE

1. Elements of proof

An electronic signature is authenticated by proof that:

a. A letter, character, number or other symbol in electronic form represents the persons named in or attached to or logically associated with an electronic data message or document; or

b. That the appropriate methodology or security procedures, when applicable, were employed or adopted by such person with the intention of authenticating or approving an electronic data message or electronic document, e.g., encryption authentication; or

c. By other ways as in the case of authenticating an electronic document such as testimonial sponsorship when a witness confirms that the signature in question is really his.[28]

IX. ELECTRONIC DOCUMENTS AND THE HEARSAY RULE

Hearsay is best described as a statement, other than the one made by the declarant while testifying at the trial or hearing, offered in evidence to

[26] *Id.*

[27] ECA, §§ 14 & 15.

[28] ECA, § 11(a).

prove the truth of the matter asserted.

The hearsay rule applies only if the statement is offered "**to prove the truth of the matter asserted.**" Thus, it does not apply to an independently relevant statement, *i.e.*, a statement that has relevance to the fact in issue, regardless or independently of the truth or falsity of the matter asserted.

Therefore, if the purpose of introducing an e-mail from B is to prove that B, who does not take the witness stand, owes A P1,000,000, as A claims, then it is hearsay. But if the purpose is to prove that B made an admission against his interest, then the e-mail is not hearsay.

This admission against interest has an independent relevance under the rule on admission against interest, regardless of the truth or falsity of the matter asserted therein. Rule 132 of the Rules of Court pertinently provides:

> Sec. 26. *Admissions of a party.* – The act, declaration or omission of a party as to a relevant fact may be admitted in evidence.

Section 7 of the ECA expressly provides that the ECA does not modify any statutory rule relating to the admissibility of electronic data messages or electronic documents, except the rules relating to authentication and best evidence. Hence, the ECA does not modify the hearsay rule. If an electronic document is hearsay, it remains inadmissible in evidence notwithstanding the fact that it is in electronic form, unless it falls under any of the exceptions to the hearsay rule.

A. EXCEPTIONS TO THE HEARSAY RULE

1. The Business Records Exception

This exception is contained in Rule 132 which provides as follows:

> SEC. 43. *Entries in the course of business.* – Entries made at, or near the time of the transactions to which they refer, by a person deceased, or unable to testify, who was in a position to know the facts therein stated, may be received as *prima facie* evidence, if such person made the entries in the performance of duty and in the ordinary course of business or duty."

For this exception to apply, the entrant must be deceased or otherwise unable to testify.[29] Inability to testify contemplates that the declarant is

[29] Cangue v. Court of Appeals, 305 SCRA 579 (1999).

either dead, mentally incapacitated or physically incompetent.[30] It does not even include hostility on the part of the declarant to testify, such as when he refuses to attend a subsequent trial. It contemplates inability proceeding from a grave cause almost amounting to death, as when the witness is old and has lost his power of speech.[31] Note that mere absence from Philippine jurisdiction does not make declarant unable to testify.

The person who made the entries must have personal knowledge of the facts constituting the entries; making the entries on the basis of the bills given to the entrant is not sufficient.[32]

This exception may be illustrated in the case of the *jueteng* expose of Gov. Chavit Singson. Assuming that the ledger naming the payees of *jueteng* money is a print-out of computer-stored data which Yolly Ricaforte encoded on the basis of information she received from Gov. Singson, the computer records or print-outs may qualify as entries in the course of business, as this exception does not distinguish between legitimate or illegitimate business.[33] However, it cannot be admitted as independent evidence to prove that the named payees received *jueteng* money, as Ms. Ricaforte did not have personal knowledge of the fact of payment.[34]

In the same *jueteng* expose, assuming that the ledger is a print-out of computer-stored data that Ms. Ricaforte encoded after personally witnessing each payment, and she later left the country, would the computer print-out be admissible as independent evidence to prove the fact of payment to the persons identified therein? The answer would have to be in the negative. Since the absence of Mrs. Ricaforte from the Philippines is not "inability to testify" within the contemplation of the business record exception to the hearsay rule,[35] the computer print-out would be inadmissible.

In *IBM*, the company contended that it was its business practice to have telematic or paperless communication through the e-mail system among its employees both here and abroad. Assuming that the print-outs had been duly authenticated, could they have been admitted in evidence to

[30] Fuentes v. Court of Appeals, 253 SCRA 430 (1996).

[31] Tan v. Court of Appeals, 20 SCRA 54 (1967).

[32] PHILAMLIFE v. Capital Assurance Corporation, 72 O.G. 3941 (1975); Cangue v. Court of Appeals, 305 SCRA 579 (1999).

[33] *See e.g.* U.S. v. Foster, 711 F.2d 871, 882 & n. 6 (9th Cir. 1983) and U.S. v. Hedman, 630 F.2d 1184 (7th Cir.1980).

[34] PHILAMLIFE v. Capital Assurance Corporation, 72 O.G. 3941 (1975); Cangue v. Court of Appeals, 305 SCRA 579 (1999).

[35] Fuentes v. Court of Appeals, 253 SCRA 430 (1996).

prove the fact of tardiness and absenteeism on the part of the employee? Since the manager who sent the e-mails did not testify during the proceedings, and there was no showing he was either dead or unable to testify, the print-outs may not be received in evidence.

The Philippines does not have a counterpart of the Business Records Act which makes business records competent evidence "if the custodian or other qualified witness" testifies as to the identity of the records and the mode of their preparation, "if kept in the course of regularly conducted business activity" and "if it was the regular practice of that business activity" to make the report "at or near the time" of the transaction in question, "unless the source of the information or the method or circumstances of preparation indicate a lack of trustworthiness."

Unlike the business records exception of the hearsay rule, the Business Records Act does not require that the entrant be either be dead or unable to testify. The entrant or preparer need not appear in court to authenticate the business record.[36]

2. Official Records Exception

This exception to the hearsay rule is contained in Rule 132 which provides as follows:

> SEC. 44. *Entries in official records.* – Entries in official records made in the performance of his duty by a public officer of the Philippines, or by a person in the performance of a duty especially enjoined by law, are prima facie evidence of the facts stated therein.

To illustrate, assume that the Republic of the Philippines files a tax evasion case against A for non-filing of income tax returns from 1995-1999. Under the computer program of the BIR, all income tax filings of each and every taxpayer are encoded into its computer system. Part of the prosecution evidence is a certification from the BIR Income Tax Division stating that based on the data contained in the computer system of the BIR as evidenced by the attached computer print-out, A had filed its income tax returns only until 1994. These documents are admissible under the official records exception to the hearsay rule.[37]

[36] U.S. v. Fendley, 522 F.2d 181 (5th Cir. 1975); U.S. v. Miller, 500 F.2d 75; U.S. v. Dawson, 400 F.2d 194 (2d Cir. 1968).

[37] *See* People v. Lazaro, G.R. No. 112090, October 26, 1999; Manalo v. Robles Transportation Co., Inc., 52 O.G. 5797 (1956).

Significantly, for this exception to apply, the entrant must have personal knowledge of the facts entered.[38]

For example, A is accused of murdering B. Part of the prosecution evidence is a police report of the incident, digitally signed by the police officer, reporting interviews of eyewitnesses who all pointed to A as the culprit of the crime. The police report cannot be admitted as independent evidence to prove A's guilt, without presenting the eyewitnesses in court. The report does not qualify as an official record admissible in evidence under the official record exception because the entrant (police officer) did not have personal knowledge of the incident reported.[39]

X. THE ECA AND THE PAROL EVIDENCE RULE

A. PAROL EVIDENCE RULE

This rule is contained in Rule 130 of the Revised Rules of Court in this wise:

> SEC. 9. *Evidence of written agreements.* – When the terms of an agreement have been reduced to writing, it is considered as containing all the terms agreed upon and there can be, between the parties and their successors in interest, no evidence of such terms other than the contents of the written agreement.
>
> However, a party may present evidence to modify, explain or add to the terms of the written agreement if he puts in issue in his pleading:
>
> a) An intrinsic ambiguity, mistake or imperfection in the written agreement;
> b) the failure of the written agreement to express the true intent and agreement of the parties thereto;
> c) the validity of the written agreement; or
> d) the existence of other terms agreed to by the parties or their successors in interest after the execution of the written agreement.
>
> The term "agreement" includes wills. (underscoring supplied)

While the ECA authorizes parties to enter into contracts electronically, it is essential that said contract complies with the requirements prescribed by law for a valid contract before an electronic document attains the status

[38] Caltex v. Africa, 16 SCRA 448 (1968).

[39] *Id.*

of a contract. Until that time, the electronic document is not covered by the parol evidence rule. As observed, "**[t]he requirement that data be presented in written form xxx should not be confused with the more stringent requirements of "signed writing", "signed original" or "authenticated legal act."**[40]

But, once an electronic document attains the status of a binding contract, the ECA provides that "**it shall be the best evidence of the agreement and transaction contained therein.**"[41] In other words, it is, for all intents and purposes, the written agreement between the parties. Thus, parol evidence cannot be introduced to vary or modify its terms, unless allowed by the parol evidence rule.

XI. EVIDENTIAL WEIGHT OF ELECTRONIC DOCUMENTS

Under the law on evidence, there is a distinction between admissibility and weight of evidence. Evidence is admissible when it fulfills the requirements of admissibility or has not been objected to, but without necessarily meaning that it will be given probative value. Admissibility is determined by law or the rules on evidence; weight is determined by the court.

Section 12 of the ECA provides that in "assessing the evidential weight of an electronic data message or electronic document, the reliability of the manner in which it was generated, the reliability of the manner in which its originator was identified, and other relevant factors shall be given due regard."

In *IBM*, assume that the computer print-outs were properly authenticated, and that the dismissed employee's supervisor, who had personal knowledge of his absences and tardiness, testified in support of his e-mails. If there was evidence that the computer data was tampered with and the supervisor's testimony was inconsistent in material details, the court could properly choose not to give any evidentiary weight to the e-mails as proof of the absences and tardiness.

[40] *See* UNCITRAL Enactment Guide, *supra* note 6.

[41] ECA, § 12[b].

XII. SOME PRACTICAL TIPS FOR PRESENTING/ IMPEACHING COMPUTER-STORED RECORDS

A. LAYING THE FOUNDATION

When presenting an electronic document, the following should be done:

1. Prove the familiarity of the witness with the computer system;

2. Establish the reliability and trustworthiness of the data or information put into the computer, *e.g.*:

   a. Describe the nature of the information which went into the machine and upon which the print-out was based;[42]

   b. Describe the nature of the information which went into the machine and upon which the print-out was based;[43]

   c. The data were reviewed and audited for errors;[44]

   d. The data stored in the system were not or could not have been tampered with before they were printed out.

3. Describe the process or system that produces the result and show that the process or system produces an accurate result, *e.g.*:

   a. The computer was tested for internal programming errors on a periodic basis;[45]

   b. The system was operating in a manner that did not affect the integrity of the electronic document or electronic data message; and
   c. There are no reasonable grounds to doubt the integrity of the computer system.

4. Describe the input and output procedures, including controls, tests and checks for accuracy;

[42] U.S. v. Russo, 480 F.2d 1228 (6th Cir. 1973).

[43] *Id.*

[44] U.S. v. Croft, 750 F.2d 1354 (C.A. Wis. 1984).

[45] U.S. v. Weatherspoon, 581 F. 2d 595 (7th Cir. 1978).

5. Establish use of computerized records in the ordinary course of business;

6. The electronic document remained complete and unaltered apart from the addition of any endorsement and any change which arises in the normal course of communication, storage and display;

7. Origin of the electronic document;

8. The computer print-out accurately reflects the data stored in the computer; and

9. If appropriate, that the computer-generated document was recorded or stored by the adverse party or a third party not under the control of the proponent.

B. IMPEACHING COMPUTER-GENERATED RECORDS

This can be done by questioning, among others:

1. The source of the input data or information;[46]

2. The process for transcribing the input data into the computer;

3. The computer programs that create, edit and update the files;[47]

4. The computer programs that produce the output or stored files;[48]

5. The reliability of the hardware and the vendor-supplied "off-the-shelf" software that systematically manages the internal processes of the computer;

6. Failure to comply with or lack of security mechanisms;

7. Tampering of the contents of the electronic document;

8. Authenticity of the electronic signatures;

9. Origin or receipt of the computer information.

[46] *See e.g.* Perma Research v. Singer Co., 542 F.2d 111 (2d Cir. 1976).

[47] *Id.*

[48] *Id.*

AN OVERVIEW OF THE E-COMMERCE ACT OF 2000

SEN. RAMON B. MAGSAYSAY, JR.

I. INTRODUCTION

Information technology is described by the World Bank as a "major opportunity for developing countries that can access and use it effectively and a threat to those that cannot." Meanwhile, North America dominates the 60 million internet users worldwide with a 68% majority or 40 million users. By default, global businesses are effectively conducted along Western arrangements. The necessary substructure commerce, such as the disciplines of banking, accounting, taxation, education, and especially information technology, is largely derived from Western practices.

By 2002, however, when the number of users are expected to increase to 228 million, the ration will also change. 143 million or 62% of users will come from outside the United States and Canada. Already, 30% of "hits" from the top ten web sites in the United States come from outside the United States, evidencing the global reach of the internet. The potential of the Internet is a challenge to a developing nation such as the Philippines.

For this potential to be realized fully, governments must adopt a non-regulatory, market-oriented approach to electronic commerce: one that facilitates the emergence of a transparent and predictable legal environment to support global business and commerce. Official decision-makers must respect the unique nature of the medium and recognize that widespread competition and increased consumer choice should be the defining features of the new digital marketplace.[1]

Cite as 45 ATENEO L.J. 377 (2001).

* Senator Ramon B. Magsaysay, Jr. is the author of the Senate Bill No. 1902, which was consolidated with House Bill No. 9971 to become the E-Commerce Act of 2000. The Ateneo Law Journal thanks Atty. Sofronio Larcia, Chief of Staff of the Office of Senator Magsaysay, for his assistance in soliciting this note. The author also wishes to acknowledge Ms. Amanda Carpo and Ms. Margaux Salcedo for their contributions to this work.

1 A Framework For Global Electronic Commerce, former President William J. Clinton and former Vice President Albert Gore, available at <http://www.ecommlaw.com> (accessed 2 April 2000).