E-DISCOVERY IN THE PHILIPPINES

by JJ Disini and Michael Anthony C. Dizon

Although the Philippines does not have special or extensive rules on e-discovery, procedural rules adopted by the Supreme Court, particularly the Rules of Civil Procedure and the Rules on Electronic Evidence ("REE"), and statutes like the Electronic Commerce Act[1] ("ECA" or the "Act") provide a basic yet workable legal framework for the conduct of e-discovery processes in the country.

The Electronic Commerce Act

Origins. The Act traces its roots to the UNCITRAL Model Law (the "Model Law") and Singapore's Electronic Transactions Act ("ETA"). The Model Law was drafted and adopted by UNCITRAL on December 16, 1996 with the intention of achieving a harmonized legal framework for electronic commerce across multiple borders. The Model Law, as the name implies, was drafted with the intention of being adopted as legislation in various countries around the world. Hence, it was written with a view to maximize acceptability in various legal systems while minimizing any adverse inconsistencies across various jurisdictions. The driving force behind the Model Law was the conviction that a secure legal environment supportive of e-commerce would lead to its promotion and growth.

Singapore's ETA is likewise based upon the Model Law. The ETA was used as a reference for the Act largely because of its provisions on digital signatures, regulation of certification authorities, and service provider liability. However, the provisions on digital signatures and the regulation of certification authorities were abandoned by the Philippine Congress. This was deemed necessary since the complexity of the underlying issues relating to asymmetric cryptosystems threatened to delay the passage of the Act. It was also recognized that digital signature legislation would be premature since no certification authority was operating in the country at that time.

Necessity for the Act. In the months leading to the passage of the Act, members of the legal profession debated on the necessity of passing legislation on electronic commerce. On the one hand, there were those who believed that such legislation would be useful to fill

[1] Republic Act No. 8792 (2000).

in some gaps in Philippine law requiring certain contracts be in "writing" (*e.g.*, statute of frauds) or that some documents be "signed" (*e.g.*, negotiable instruments). There were even those who believed that all electronic commerce transactions would be void and invalid without such a law. At the other end of the spectrum were those who did not see the necessity for the Act and argued that since the law already recognizes verbal or oral agreements, there should be no reason why electronic contracts would be denied validity. Nevertheless, there remained unanswered questions such as: *Should electronic documents be given the same status as paper documents? Do electronic signatures enjoy the same validity and authenticity as manually signed signatures?*

Before the advent of the Act, Philippine statutory law did not categorically validate electronic evidence. There is likewise no validation under Philippine jurisprudence since the courts had no real opportunity to rule on this matter. The only related case is the one recently decided by the Supreme Court where it declared electronic mail inadmissible due largely to the fault of the offering party, who merely printed out the messages without having them authenticated or certified as accurate.[2] Under these circumstances, even if the evidence *were* in the form of paper documents, they would be inadmissible for lack of proper authentication. Nevertheless, this case left an indelible and erroneous impression that electronic evidence was inadmissible.

To make matters worse, it was universally acknowledged that the resolution of legal issues respecting the validity of electronic contracts and the admissibility of electronic evidence would take years or even decades if left in the hands of the Philippine judiciary. This springs mainly from the fact that the only source of binding case law in the Philippines are decisions of the Supreme Court. Meanwhile, in the absence of any existing legal framework for electronic commerce, the law would, at best, be in a state of flux which would very well be a hindrance to the promotion of electronic commerce in the country.

The brewing debate among lawyers and judges only highlighted the fact that there was at the very least a *doubt* respecting the validity of e-commerce transactions. Unfortunately, the absence of a clear consensus among legal experts only created an atmosphere of uncertainty especially among those in the business community. Such uncertainty in turn brought fear, which stifled investment and entrepreneurship as businessmen readily dismissed e-commerce as an all-too risky endeavor. The only solution

[2] *IBM Philippines, Inc. v. NLRC*, 305 SCRA 592 [1999].

to the conundrum therefore, was to pass the Electronic Commerce Act and expressly recognize, in no uncertain terms, that doing business electronically is *legal, valid and enforceable in a court of law.*

Guiding Principles of the Act. The primary guiding principle behind the Act is the ***"****functional equivalent"* approach. Under this approach, the *functions* of a document or a signature are analyzed, and, if an *equivalent* exists in electronic form, then the latter will be adopted. For example, a signature performs the function of identifying the signer and indicating his consent to a document. If an electronic method performs the same functions, then such method would be considered an electronic signature.

Apart from the "functional equivalent" approach, the Act is likewise technology-neutral since it does not favor any particular technology. It has long been recognized that laws that are not technology-neutral trigger market distortions and impact against competing technologies. Moreover, a technology-specific statute would encourage the private sector to support only that technology and establish it as a single or sole standard. If this persists, it will inevitably result in a dearth of innovation and inventiveness, as all resources will be devoted to sustain the favored technology. To avoid this, the Act was written with an overriding concern to embrace the full range of electronic technology without bias or prejudice. Thus, the Act does not discriminate among any type of electronic document or signature utilizing a particular technology. At most, the Act specifies standards and criteria for electronic documents and signatures but the same are written in a manner that does not favor any specific technology. In fact, the Act admits all types of security measures and leaves parties free to determine the type and level of security needed for their transactions. It also allows parties to select the appropriate technological methods that will suit their needs.

A necessary adjunct to technology neutrality is the principle of media neutrality that is likewise ingrained in the Act. In sum, the Act recognizes electronic documents and signatures in whatever media they may be found. For example, if an electronic message is received both as an electronic mail and fax, both of them will be considered an electronic data message or electronic document.

Media neutrality is also an important principle inasmuch as electronic data routinely changes its form in the course of transmission. A text or SMS message, for example, may be transmitted as Internet e-mail and received by the addressee as a fax message. Media

neutrality ensures no discrimination in the legal treatment of the electronic document from the time of its creation or delivery to the time of its receipt or acceptance.

Role of the Act vis-à-vis Philippine Law. The Act was not intended nor designed to supplant any substantive law, particularly the law on contracts. Moreover, except for the new crimes punishable under the Act, activities that were lawful or unlawful, retained the same status prior to the passage of the Act. The Act principally affected the *form* of transactions and activities by recognizing electronic documents and signature without affecting their underlying legal validity. In other words, Philippine substantive law continued to apply to all e-commerce transactions.

Salient Features. In a nutshell, the Act:

- Raises electronic documents to the same legal status as paper documents;
- Elevates electronic signatures to the level of manually-signed signatures;
- Allows the use of electronic documents and electronic signatures in commercial and non-commercial transactions;
- Mandates the Government to conduct its business electronically within two (2) years; and,
- Criminalizes hacking and on-line piracy.

Electronic Documents. The Act simply states that information in electronic documents will not be denied legal effect on the sole ground that it is in electronic form. Note that the law does not intend to validate the *contents* of electronic documents but only their *form*.

In practical terms, whenever the Act requires a "writing" or a "document", an electronic document will suffice. However, it should be noted that if a notarized document is required by law (such as in a special power of attorney to sell land), such a document may not be in electronic form until the Supreme Court promulgates rules on electronic notarization.

Moreover, information in electronic documents may be given effect even if it does not appear in the document but is merely referred to therein. This facilitates the use of codes in electronic contracts or the incorporation of standard terms and conditions by way of an active

hyperlink. Finally, the Act allows records required by the government to be kept in electronic form – a first in Philippine law.

Electronic Signatures. It is commonly believed that electronic signatures are confined to graphic representations of manually-signed signatures. This, of course, is a fallacy. An electronic signature may be any distinctive mark that represents the identity of a person and is intended to authenticate or approve a document. The definition is, of course, taken from the real world function of a signature. Under the Act if a person were to write the following words in an e-mail: "Okay. Sgd. Gloria" – that would be a sufficient electronic signature. However, Section 8 of the Act seems to require a particular non-alterable process before an electronic signature is given legal effect and validity. Because Section 8 was taken from various sources, including the Singapore ETA, it seems that the only technology that qualifies as a valid electronic signature are digital signatures which are issued within the broader context of a public key infrastructure. All other electronic signatures would, generally, be invalid under Philippine law. Thankfully, Philippine contract law adheres to the spiritual system whereby contracts as a general proposition are valid in any form they may be found. This means that the restrictive approval of electronic signatures under the Act does not largely affect the validity of electronic contracts where the form of the consent is expressed through means other than digital signatures.

Scope of the Law. Despite its title, the "Electronic Commerce Act" applies equally to non-commercial transactions. The expansion of its scope was necessary in order to allow electronic documents to perform non-commercial functions such as establishing the paternity of a child, casting a vote in an election, and committing torts and criminal offenses (*e.g.*, libel and threats).

The Rules on Electronic Evidence.

In 2001, the Supreme Court issued the Rules on Electronic Evidence ("REE"), which sought to fill-in the gaps in Philippine procedural rules that did not explicitly provide for the admissibility of electronic evidence. It was also important for the Court to emphasize that as a matter of evidence, there should be no discrimination between the treatment of electronic and other types of evidence.

Guiding Principles. The REE integrates the ECA's adoption of the functional equivalence principle, as well as its principle of non-discrimination against electronic documents, in determining admissibility in evidentiary proceedings.

The REE implements Section 7 of the ECA which provides that "(f)or evidentiary purposes, an electronic document shall be the functional equivalent of a written document under existing laws." Consequently, electronic documents and electronic data messages are documentary evidence under the Rules of Court that require documentary evidence to be subject to a process of authentication by a witness, prior to admission as evidence. Similarly, the REE provides for methods of authentication specific for electronic documents and in the same light, the REE requires that electronic documentary evidence be sponsored by a witness that authenticates the same.

Best Evidence Rule. The Philippine legal system adopts the "best evidence" rule, which requires that the "originals" of the documents be presented for certain assertions of facts. The ECA expanded this rule by stating that legal requirements for the originals are "met by an electronic data message or electronic document", as follows:

a. The integrity of the information from the time when it was first generated in its final form as an electronic data message or electronic document is shown; and
b. That the information is capable of being displayed to the person to whom it is to be presented.[3]

The same provisions of the ECA provide that the integrity of the electronic document shall be assessed based on:

a. Whether the information 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

[3] *Republic Act 8792 - Electronic Commerce Act*, sec. 10.

b. The standard of reliability required shall be assessed in the light of the purpose for which the information was generated and in the light of all relevant circumstances.[4]

The REE effectively amends the Best Evidence Rule in providing that "(a)n electronic document shall be regarded as the equivalent of an original document" if:

a. It is a printout or output readable by sight or other means;
b. It is shown to reflect the data accurately.

The same Rule enables the presentation of duplicate originals or copies "executed at or about the same time with identical contents" or counterparts. These duplicates shall also be considered as equivalent of an original.[5]

In *MCC Industrial Sales v. Ssangyong*, the Philippine Supreme Court adopted the view that the original print-out from a fax machine or its subsequent photocopies are not electronic data messages or electronic documents[6], and therefore refused to apply the said rule on duplicate originals. Instead, the SC ruled that the original documents – not the fax copies, should be presented in evidence.

Given the variance in the Best Evidence Rule in the Rules of Court and the REE, the status of the document as either electronic or paper-based, determines the form of the evidence that is admissible in court. As stated earlier, duplicate originals (such as print-outs or photo copies) would suffice for electronic documents but not for paper documents.

The separate treatment of paper and electronic documents however can be addressed by the integration of the REE into the Rules of Court. Consequenlty, paper and electronic documents will fall under a single category: documentary evidence.

Authentication of Electronic Documents. Rule 5 of the REE mirrors the text of the ECA in establishing that the party who seeks to introduce an electronic document in any legal proceeding has the burden of proving its authenticity by evidence capable of supporting the relevant point of fact, i.e., that the electronic document is what the party making the

[4] Ibid.
[5] *A.M. 01-7-01-SC 2001-07-17 - Rules on Electronic Evidence*, *AM*, 2001, sec. 1.
[6] MCC Industrial Sales Corporation V. Ssangyong Corporation, G.R. No. 170633, October 17, 2007.

assertion claims it to be. Failure to authenticate under Rule 5 of the REE means that an electronic document cannot be admitted into evidence.[7]

The REE provides three modes through which an electronic document may be authenticated. According to Rule 5, authenticity may be established by presenting:

a. Evidence that the electronic document has been digitally signed;
b. Evidence that other appropriate security procedures or devices as may be authorized by the Supreme Court or by law for authentication of electronic documents were applied to the document; and
c. Evidence showing its integrity and reliability to the satisfaction of the judge.[8]

In the case of *Aznar v. Citibank*, where a print out purported to originate from a computer system was involved, the Supreme Court interpreted the authentication requirement for electronic documents as a duty of the proponent to "demonstrate how the information reflected in the print-out was generated and how the said information could be relied upon as true."[9]

Weight and Sufficiency of Electronic Evidence. Separate from the issue of admissibility after the electronic evidence has been duly authenticated is the issue of evaluating the probative weight of electronic documents admitted into evidence. The REE puts forward the following factors for consideration of the court:

a. The reliability of the manner or method in which it was generated, stored or communicated, including but not limited to input and output procedures, controls, tests and checks for accuracy and reliability of the electronic data message or document, in the light of all the circumstances as well as any relevant agreement;
b. The reliability of the manner in which its originator was identified;

[7] Ibid. Rule 5, sec. 1.
[8] Ibid. Rule 5, sec. 2.
[9] *Emmanuel Aznar V. Citibank N.A.* (2007).

c. The integrity of the information and communication system in which it is recorded or stored, including but not limited to the hardware and computer programs or software used as well as programming errors;
d. The familiarity of the witness or the person who made the entry with the communication and information system;
e. The nature and quality of the information which went into the communication and information system upon which the electronic data message or electronic document was based; or
f. Other factors which the court may consider as affecting the accuracy or integrity of the electronic document or electronic data message.[10]

For evaluating the integrity of an information and communication system at this stage, the REE likewise provides the following factors for consideration:

a. Whether the information and communication system or other similar device was operated in a manner that did not affect the integrity of the electronic document, and there are no other reasonable grounds to doubt the integrity of the information and communication system;
b. Whether the electronic document was recorded or stored by a party to the proceedings with interest adverse to that of the party using it; or
c. Whether the electronic document was recorded or stored in the usual and ordinary course of business by a person who is not a party to the proceedings and who did not act under the control of the party using it.[11]

Other Electronic Evidence. The REE also provides for the admissibility of audio, photographic and video evidence. It enables the presentation of the so-called ephemeral electronic communication - electronic documents that are routinely destroyed after their transmission, such as text messages or emails. In all cases, where these pieces of evidence are presented, they must be authenticated by the testimony of a witness.

[10] Ibid., Rule 7, sec. 1.
[11] Ibid., Rule 7, sec. 2.

In addition, the REE provides for the admissibility of electronic business records[12] and permits their entry into evidence in judicial proceedings upon the testimony of the custodian or other qualified witnesses. This represents a departure from the rules of evidence governing paper-based records which may be admitted if they are authenticated by the person who has actual knowledge of the facts stated therein, and only upon the latter's death or unavailability will the courts allow the records to be admitted as proof of their contents[13]. In this case, the REE establishes a bias in favor of electronic records in the sense that they are more easily presented into evidence in court.

The Rules on Discovery

The Rules of Court provide for different modes of discovery such as depositions pending actions, depositions before action or pending appeal, interrogatories to parties, admission by adverse party, physical and mental examination of persons, and production or inspection of documents or things.[14] As a general proposition, once the parties have exchanged their pleadings at the initial stage of the litigation, they may engage in all forms of discovery without requiring the approval of the trial court. Indeed, all modes of discovery occur outside the courts themselves and judges participate only when they are called upon to intervene if a party engages in unfair or illegal acts while availing of such remedies.

Depositions and Interrogatories. The Rules of Court allow all parties to a suit to call *any witness* to testify in a deposition or through written interrogatories, in *any matter* that is relevant to a pending action. In fact, the Supreme Court has gone so far as to categorically allow a deposition or the modes of discovery to be used by a party to engage in a fishing expedition[15].

Requests for Admission. A party to a suit may file upon the other party, a request for an admission of the genuineness of any material and relevant document or any fact indicated in the request. Unless the receiving party specifically denies the matter in the request and sets forth the truth, the subject matter of the request is deemed admitted and may be used in the pending action between them.

[12] Ibid., Rule 8, secs. 1 & 2.
[13] ROC, Rule 130, sec. 43.
[14] Rules of Civil Procedure, Rules 23-29.
[15] Republic v. Sandiganbayan, G.R. No. 90478, November 21, 1991.

Physical and Mental Examination of Persons. Whenever the mental or physical condition of a party is in controversy, a party may require the court to cause the examination of such party by a physician. While the report will go to the requesting party, the one examined is also entitled to a copy of the report.

Production of Documents. The rule on production and inspection orders states:

> Upon motion of any party showing good cause therefor, the court in which an action is pending may (a) order any party to produce and permit the inspection and copying or photographing, by or on behalf of the moving party, of any designated documents, papers, books, accounts, letters, photographs, objects or tangible things, not privileged, which constitute or contain evidence material to any matter involved in the action and which are in his possession, custody or control…. The order shall specify the time, place and manner of making the inspection and taking copies and photographs, and may prescribe such terms and conditions as are just.[16]

Under this Rule, it is the order of the court that specifically sets out and determines the scope and extent of the electronic documents to be produced as part of e-discovery. The coverage and the terms and conditions of the production or inspection order, are therefore decided by the court on a case-by-case basis, bearing in mind the particular facts and circumstances of the case. The issuance of a production or inspection order is subject to the requirements that, (1) it be made upon the "showing of good cause" by the moving party; (2) it excludes privileged information; and (3) the documents sought to be produced must "constitute or contain evidence material to any matter involved in the action".[17] In any event, the production or inspection order must be clearly delimited in terms of time, place and manner and its terms and conditions must be just and not unduly burdensome on the producing party.[18] For example, in the case of *Aznar v Citibank*, which involved the admissibility of computer printouts concerning the status of the plaintiff's credit card,[19] the plaintiff cardholder could have resorted to Rule 27 to compel the bank to produce electronic documents relating to the alleged "blacklisting" of his credit card by the bank. While the bank itself did produce some relevant electronic documents and business records to successfully prove its case,[20] the plaintiff could have requested the production of these and

[16] Rules of Civil Procedure, Rule 27.
[17] Rules of Civil Procedure, Rule 27.
[18] Rules of Civil Procedure, Rule 27.
[19] *Aznar v Citibank*, G.R. No. 164273 [March 28, 2007].
[20] *Aznar v Citibank*, G.R. No. 164273 [March 28, 2007].

other pertinent documents as part of discovery and could not have been limited to those offered by the bank in evidence.

Penalties for Failure to Comply with Discovery Modes. There are serious consequences for failing or refusing to comply with a production or inspection order. Rule 29 section 3 of the Rules of Civil Procedure states that "[i]f any party or an officer or managing agent of a party refuses to obey… an order under Rule 27 to produce any document or other thing for inspection, copying, or photographing… the court may make such orders in regard to the refusal as are just". The court may, among other things, issue orders that: (1) state that the matters regarding… the contents of the paper… or any other designated facts shall be taken to be established for the purpose of the action in accordance with the claim of the party obtaining the order;" (2) refuse to allow the disobedient party to support or oppose designated claims or defenses or prohibit him from introducing in evidence designated documents or things; (3) strike out pleadings or parts thereof, or stay further proceedings until the order is obeyed, or dismiss the action or proceeding or any part thereof, or render a judgment by default against the disobedient party;" and (4) "[i]n lieu of any of the foregoing orders or in addition thereto, an order directing the arrest of any party or agent of a party for disobeying any of such orders except an order to submit to a physical or mental examination".[21]

Electronic Discovery

While the discovery rules as discussed, originally contemplated paper or physical documents, they equally apply to electronic documents and other digital messages and data. This is the implication of the subsequent enactment of the Electronic Commerce Act, which is the main law that provides legal recognition of electronic documents, electronic data messages and electronic signatures.[22] The Act states: "[e]lectronic documents shall have the legal effect, validity or enforceability as any other document or legal writing"[23] and "[i]nformation shall not be denied validity or enforceability solely on the ground that it is in the form of an electronic data message purporting to give rise to such legal effect, or that it is merely incorporated by reference in that electronic data message.[24] An "electronic document" is defined under the law as:

[21] Rules of Civil Procedure, Rule 29 sec 3.
[22] Electronic Commerce Act, secs 6, 7 and 8.
[23] Electronic Commerce Act, sec 7.
[24] Electronic Commerce Act, sec 6.

> "…information or the representation of information, data, figures, symbols or other modes of written expression, described or however represented, by which a right is established or an obligation extinguished, or by which a fact may be proved and affirmed, which is received, recorded, transmitted, stored, processed, retrieved or produced electronically."[25]

The term "electronic data message" covers any "information generated, sent, received or stored by electronic, optical or similar means".[26] An "electronic signature" on the other hand 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."[27]

According to the Supreme Court:

> " . . . what differentiates an electronic document from a paper-based document is the manner by which the information is processed; clearly, the information contained in an electronic document is received, recorded, transmitted, stored, processed, retrieved or produced electronically."[28]

In this case, the Court ruled that photocopies of what were originally paper documents are not electronic documents.[29] It should also be noted that, in contrast to the UNCITRAL Model Law on Electronic Commerce, the Supreme Court has ruled that "a facsimile transmission cannot be considered as electronic evidence. It is not the functional equivalent of an original under the Best Evidence Rule and is not admissible as electronic evidence".[30]

In relation to procedural rules, the Electronic Commerce Act specifically provides that: "(f)or evidentiary purposes, an electronic document shall be the functional equivalent of a written document under existing laws".[31] Further, with regard to the "admissibility and evidential weight" of electronic documents and data messages, the Act states that "[i]n any legal proceedings, nothing in the application of the rules on evidence shall deny the

[25] Electronic Commerce Act, sec 5(f).
[26] Electronic Commerce Act, sec 5(c).
[27] Electronic Commerce Act, sec 5(e).
[28] *National Power Corporation v Codilla*, G.R. No. 170491 [April 3, 2007].
[29] *National Power Corporation v Codilla*, G.R. No. 170491 [April 3, 2007].
[30] *MCC Industrial Sales Corporation v Ssangyong Corporation*, G.R. No. 170633 [October 17, 2007]; see also *Torres v Philippine Amusement and Gaming Corporation*, G.R. No. 193531 [December 6, 2011].
[31] Electronic Commerce Act, sec 7.

admissibility of an electronic data message or electronic document in evidence… [o]n the sole ground that it is in electronic form".[32]

Moreover, the Rules on Electronic Evidence clearly states that "(w)henever a rule of evidence refers to the term writing, document, record, instrument, memorandum or any other form of writing, such term shall be deemed to include an electronic document as defined in these Rules."[33] While the rules on the modes of discovery are not located within the rules on evidence, clearly the discovery rules speak of evidentiary matters and therefore, those discovery rules will apply to electronic documents or electronic data messages.

Lastly, the retention and presentation of electronic documents and data messages are very relevant to the subject of e-discovery. The law stipulates that:

> (1) Where the law requires information to be presented or retained in its original form, that requirement is met by an electronic data message or electronic document if:
>
> (a) the integrity of the information from the time when it was first generated in its final form, as an electronic data message or electronic document is shown by evidence *aliunde* or otherwise; and
>
> (b) where it is required that information be presented, that the information is capable of being displayed to the person to whom it is to be presented.[34]

A document is considered contained in its original form if it: (1) "[r]emains accessible so as to be usable for subsequent reference;" (2) "[i]s retained in the format in which it was generated, sent or received, or in a format which can be demonstrated to accurately represent the electronic data message or electronic document generated, sent or received;" and (3) "[e]nables the identification of its originator and addressee, as well as the determination of the date and the time it was sent or received".[35] A court may therefore compel a party to produce such electronic documents and data in its possession, control or custody pursuant to a production or inspection order.

In addition to the Electronic Commerce Act, the Rules on Electronic Evidence are especially relevant to e-discovery. It is worth noting that these rules apply in "civil actions and proceedings, as well as quasi-judicial and administrative cases", and also in criminal

[32] Electronic Commerce Act, sec 12.
[33] Rules on Electronic Evidence, rule 3, sec 1.
[34] Electronic Commerce Act, sec 10(1).
[35] Electronic Commerce Act, sec 13(a).

actions.[36] The rules expressly recognize that an electronic document is a "functional equivalent of paper-based documents".[37] Electronic documents are admissible in evidence as long as they comply "with the rules on admissibility prescribed by the Rules of Court and related laws, and is authenticated in the manner prescribed by these Rules".[38] It should be emphasized that, under these rules, the "confidential character of a privileged communication is not lost solely on the ground that it is in the form of an electronic document".[39] This means that documents, papers and information covered by, for instance the attorney-client privilege, remain protected even if they are in electronic form or format.

Under the Rules on Electronic Evidence, "[a]n electronic document shall be regarded as the equivalent of an original document covered by the Best Evidence Rule, if it is a printout or output readable by sight or other means, shown to reflect the data accurately".[40] Thus, a party who is required to produce documents pursuant to a production order may provide electronic and/or printed copies of the documents requested. According to the rules, a "person seeking to introduce an electronic document in any legal proceeding has the burden of proving its authenticity".[41] Discovery procedures are legal proceedings and are thus covered by these rules.

The authenticity of an electronic document or data message may be proved:

> (a) by evidence that it had been digitally signed by the person purported to have signed the same;
> (b) by evidence that other appropriate security procedures or devices as may be authorized by the Supreme Court or by law for authentication of electronic documents were applied to the document; or
> (c) by other evidence showing its integrity and reliability to the satisfaction of the Judge.[42]

Electronic signatures can be authenticated:

> (a) By evidence that a method or process was utilized to establish a digital signature and verify the same;
> (b) By any other means provided by law; or
> (c) By any other means satisfactory to the judge as establishing the genuineness of the electronic signature.[43]

---

[36] Rules on Electronic Evidence, Rule 1 sec 2; *People v Enojas*, G.R. No. 204894 [March 10, 2014]; but see *Ang y Pascua v Court of Appeals*, G.R. No. 182835 [April 20, 2010].
[37] Rules on Electronic Evidence, Rule 3 sec 1.
[38] Rules on Electronic Evidence, Rule 3 sec 2.
[39] Rules on Electronic Evidence, Rule 3 sec 3.
[40] Rules on Electronic Evidence, Rule 4 sec 1.
[41] Rules on Electronic Evidence, Rule 5 sec 1.
[42] Rules on Electronic Evidence, Rule 5 sec 2.

The security and integrity of information and communication system used by a party to record, store or retain electronic documents is another consideration when determining authenticity of electronic documents produced as part of an e-discovery. As such, relevant factors to consider include:

> (a) Whether or not the information and communication system or other similar device was operated in a manner that did not affect the integrity of the electronic document, and there are no other reasonable grounds to doubt the integrity of the information and communication system;
> (b) Whether or not the electronic document was recorded or stored by a party to the proceedings with interest adverse to that of the party using it; or
> (c) Whether or not the electronic document was recorded or stored in the usual and ordinary course of business by a person who is not a party to the proceedings and who did not act under the control of the party using it.[44]

In case of "any dispute involving the integrity of the information and communication system in which an electronic document or electronic data message is recorded or stored",[45] the producing party has to show compliance with or adherence to the above factors or conditions.

Under the Rules on Electronic Evidence, electronic business records are exempt from the hearsay rule, which requires that a "witness can testify only to those facts which he knows of his personal knowledge; that is, which are derived from his own perception".[46] The term business records cover "records of any business, institution, association, profession, occupation, and calling of every kind, whether or not conducted for profit, or for legitimate or illegitimate purposes".[47] The Rules on Electronic Evidence further provide that:

> A memorandum, report, record or data compilation of acts, events, conditions, opinions, or diagnoses, made by electronic, optical or other similar means at or near the time of or from transmission or supply of information by a person with knowledge thereof, and kept in the regular course or conduct of a business activity, and such was the regular practice to make the memorandum, report, record, or data compilation by electronic, optical or similar means, all of which are shown by the testimony of the custodian or other qualified witnesses, is excepted from the rule on hearsay evidence.[48]

---

[43] Rules on Electronic Evidence, Rule 6 sec 2.
[44] Rules on Electronic Evidence, Rule 7 sec 2.
[45] Rules on Electronic Evidence, Rule 7 sec 2.
[46] Rules on Evidence, 130 sec 36.
[47] Rules on Electronic Evidence, Rule 2 sec 1(b).
[48] Rules on Electronic Evidence, Rule 8 sec 1.

Such business records may the subject of e-discovery and can be admitted in evidence in a legal proceeding by means of "an affidavit stating facts of direct personal knowledge of the affiant or based on authentic records".[49]

Conclusion

The Rules of Court while expressly permitting the modes of discovery to be used in cases, are largely unutilized by lawyers in the Philippines. Instead of engaging in discovery proceedings, they have a tendency to present all witnesses and evidence before a judge in protracted trials that take many years to litigate. In many instances, the length of time is a challenge upon because witnesses become unavailable, evidence is lost or mislaid, and memories fade.

The tendency to present all evidence before the judge takes up the court's time and is quite wasteful. In many instances, the absence of deposition proceedings may result to cross-examination questions that are not methodical and ad-hoc, with the lawyer struggling to find his footing having only considered the direct testimony. In regular court proceedings, the direct examination is held on one trial day and the cross-examination occurs months later, due to challenges in the schedule of the lawyer, coupled with having to wait for generation of the official transcript of the direct examination that is useful in his preparation for cross-examination.

This wasteful practice has been avoided to a certain degree by the new rules requiring that direct examination be conducted via a judicial affidavit served upon the other party prior to the presentation of the witness. While this rule has the effect of saving time for the trial court, it pales in comparison with the time that would have been saved by the court if the modes of discovery were properly utilized. The presentation of witnesses may be dispensed with altogether as depositions are used to support applications for summary judgment that can result in a judicial determination of key parts of a case.

This leads to a critical point about the ability of modes of discovery to secure an amicable settlement between the parties. If used properly, modes of discovery will help a party determine the actual strength or weakness of a particular claim or defense. Such realization may encourage a party to either seek settlement or cause the dismissal of a claim. Undoubtedly, the missed opportunity to settle a case because documents that may prove a claim are not produced in discovery, is a failure in the administration of justice.

[49] Rules on Electronic Evidence, Rule 9 sec 1.

In the context of e-discovery, this can be quite important. As more cases involve electronic evidence, parties need to realize that their presentation depend upon the ability of counsel to access the same. Currently, the present state of litigation in the Philippines cause lawyers to rely on the electronic documents in the possession of their client. The lack of experience in discovery means that many forms of electronic evidence like emails and text messages of the opposing party are free from the risk of being brought to court as part of a case. The increased use of cloud services also poses new challenges because the evidence may not be located within the territorial jurisdiction of the court., resulting to the cloud provider stifling a party's ability to use discovery procedures in establishing his case.

Although the Supreme Court exhorts the benefits of discovery in all types of cases, the low rate of discovery utilization by Philippine lawyers signifies that there are no relevant case law on the matter. Indeed, because Philippine lawyers typically do not concern themselves with discovery proceedings whenever they handle cases, the threat of discovery is almost non-existent. The same rings true for electronic discovery, as the lack of familiarity in discovery of real-world evidence spills over, and to large extent, creates a barrier to the use of e-discovery in many cases.

It is quite ironic that there are many e-discovery firms processing evidence in cases pending before other countries such as the United States, while those techniques are largely unheard of in the Philippines. It is hoped that a change in attitude among Philippine lawyers and the continued encouragement by the Supreme Court for the adoption of these modes of discovery will usher a new phase in the history of the Philippine legal system where e-discovery can be effectively used to champion the cause of justice in the country.