ARTICLE:

ELECTRONIC EVIDENCE AND ELECTRONIC SIGNATURES IN INDONESIA: THE PROBATIVE VALUE OF DIGITAL EVIDENCE

By **Dr. Edmon Makarim, Kom., S.H., LL.M.**

Indonesian procedural law altered slightly with the passing of Law No. 11 of 2008 Concerning Electronic Information and Transactions, and Government Regulation No. 82 of 2012. Indonesian law now provides for the probative value of electronic data to be classified as the best evidence for the purpose of legal proceedings. The probative value will be considered against the reliability of the security surrounding the data. The strongest probative value is given to digital evidence that uses digital signatures that are supported by an electronic certificate from a certified and accredited system service provider and rooted to the national or government public key infrastructure.

Introduction

Legal proceedings in Indonesia are governed by a general code for criminal proceedings (Indonesian Law No. 8 of 1981 concerning General Criminal Proceedings (KUHAP)); a general code for civil proceedings, *Het Herziene Indonesisch Reglement* (HIR) and the Fourth Book of the Indonesian Civil Code (Indonesian Burgelijk Wetbook) (KUHPer).

Indonesia also has a number of specific laws of particular criminal activities that also have their own special proceedings.[1] After the age of reformation[2] in the Indonesian legal system, many new laws were enacted that are classified as particular laws. Given the principle that where two laws govern the same facts, the law governing specific subject matter overrides the law that governs general matters,[3] specific legal provisions of a particular law might waive the general code. However, the basic principle remains that it is usual to automatically refer to the general norms of the KUHAP or HIR, unless there is a particular law that regulates specific provisions for certain facts.

Unfortunately, there are no explicit provisions that mention electronic evidence in the KUHAP or HIR. Therefore legal scholars continue to debate the extent that the present procedural laws acknowledge electronic evidence. Some scholars consider the existing laws do not cover electronic evidence because of the limitation principles of the existing legal provisions. On the other hand, other scholars think that it is possible to acknowledge electronic evidence by interpretation or widening the scope of the existing legal evidence to accommodate electronic evidence.[4]

This dualism of thinking occurred before the enactment of Law 11 of 2008 concerning the Information and Electronic Transactions (EIT Law). Before 2008, there were a number of new laws that expressly accepted electronic information or electronic documents as evidence, but the acceptance of electronic evidence is limited only within the scope of the particular law, such as Law No. 31 of 1999, as amended by Act No. 20 of 2001 on the Eradication of Corruption:

1 *The Indonesian civil code and the civil procedural code (Indonesian Burgelijk Wetbook and HIR) were implemented quickly under the emergency situation after Indonesian Independence on 17 August 1945. The purpose of the enactment was to avoid a vacuum. Article 2 of Transitional Rules of the Indonesian Constitution 1945 provides that all state agency and existing laws and regulations are still applied directly, as long as the new law is not promulgated according to this Constitution. [Pasal 2 aturan peralihan Undang-Undang Dasar 1945: Segala Badan Negara dan Peraturan yang ada masih langsung berlaku, selama belum diadakan yang baru menurut Undang-undang Dasar ini].*

2 *The Reformation Age started after the fall of the Suharto regime in Indonesia in May 1998.*

3 *Lex specialis derogat legi generali.*

4 *The conservative opinion against digital evidence is not explicitly stated in any written academic papers of Indonesian scholars. The opinion arises explicitly in debates relating to the introduction of the EIT Law. See also footnote 9.*

Pasal 26 A

Alat bukti yang sah dalam bentuk petunjuk sebagaimana dimaksud dalam Pasal 188 ayat (2) Undang-undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana, khusus untuk tindak pidana korupsi juga dapat diperoleh dari:

(a) alat bukti lain yang berupa informasi yang diucapkan, dikirim, diterima, atau disimpan secara elektronik dengan optik atau yang serupa dengan itu; dan

(b) dokumen, yakni setiap rekaman data atau informasi yang dapat dijabat, dibaca, dan atau didengar yang dapat dikeluarkan dengan atau tanpa bantuan suatu sarana, baik yang tertuang di atas kertas, benda fisik apapun selain kertas, maupun yang terekam secara elektronik, yang berupa tulisan, suara, gambar, peta, rancangan, foto, huruf, tanda, angka, atau perforasi yang memiliki makna.

Article 26 A

Valid evidence in the form of the information referred to in Article 188 paragraph (2) of Law No. 8 of 1981 on Criminal Proceedings, Special to Corruption can also be obtained from:

(a) other evidence in the form of spoken information, sent, received, or stored electronically with optical disk or similar with it, and

(b) documents, any recorded data or information that can be held, read, or heard and which can be removed with or without the help of an instrument, whether on paper, physical objects other than paper, or recorded electronically, in the form of writing, sound, images, maps, plans, photographs, letters, signs, figures, or perforations having meaning.

Meanwhile, other laws might expressly provide for electronic evidence as a new category outside of the existing categories, such as: Law No. 15 of 2003 concerning Stipulation of Government Regulation in Lieu of Law No. 1 of 2002 on Combating Criminal Acts of Terrorism Becomes Law (Terrorism Act); Law No. 15 of 2002 on the Money Laundering Criminal Act (Money Laundering Act), and Law No. 21 of 2007 on Human Trafficking (Human Trafficking Act).

UU Tindak Pidana Pencucian Uang (2002)	UU Pemberantasan Tindak Pidana Terorisme (2003)	UU Tindak Pidana Perdagangan Orang (2007)
Pasal 1 angka (7) Dokumen adalah data, rekaman, atau informasi yang dapat dilihat, dibaca, dan/atau didengar, yang dapat dikeluarkan dengan atau tanpa bantuan suatu sarana, baik yang tertuang di atas kertas, benda fisik apapun selain kertas, atau yang terekam secara elektronik, termasuk tetapi tidak terbatas pada: a. tulisan, suara, atau gambar; b. peta, rancangan, foto, atau sejenisnya; c. huruf, tanda, angka, simbol, atau perforasi yang memiliki makna atau dapat dipahami oleh orang yang mampu membaca atau memahaminya. Pasal 38 Alat bukti pemeriksaan tindak pidana pencucian uang berupa: a. alat bukti sebagaimana dimaksud dalam Hukum Acara Pidana; b. alat bukti lain berupa informasi yang diucapkan, dikirimkan, diterima, atau disimpan secara elektronik dengan alat optik atau yang serupa dengan itu; dan c. dokumen sebagaimana dimaksud dalam Pasal 1 angka 7.	Pasal 27 UU 15/2003 on terrorism Alat bukti pemeriksaan tindak pidana terorisme meliputi: a. alat bukti sebagaimana dimaksud dalam Hukum Acara Pidana; b. alat bukti lain berupa informasi yang diucapkan, dikirimkan, diterima, atau disimpan secara elektronik dengan alat optik atau yang serupa dengan itu; dan c. data, rekaman, atau informasi yang dapat dilihat, dibaca, dan/atau didengar, yang dapat dikeluarkan dengan atau tanpa bantuan suatu sarana, baik yang tertuang di atas kertas, benda fisik apapun selain kertas, atau yang terekam secara elektronik, termasuk tetapi tidak terbatas pada: 1) tulisan, suara, atau gambar; 2) peta, rancangan, foto, atau sejenisnya; 3) huruf, tanda, angka, simbol, atau perforasi yang memiliki makna atau dapat dipahami oleh orang yang mampu membaca atau memahaminya.	Pasal 29 Alat bukti selain sebagaimana ditentukan dalam Undang-Undang Hukum Acara Pidana, dapat pula berupa: a. informasi yang diucapkan, dikirimkan, diterima, atau disimpan secara elektronik dengan alat optik atau yang serupa dengan itu; dan b. data, rekaman, atau informasi yang dapat dilihat, dibaca, dan/atau didengar, yang dapat dikeluarkan dengan atau tanpa bantuan suatu sarana, baik yang tertuang di atas kertas, benda fisik apa pun selain kertas, atau yang terekam secara elektronik, termasuk tidak terbatas pada: 1) tulisan, suara, atau gambar; 2) peta, rancangan, foto, atau sejenisnya; atau 3) huruf, tanda, angka, simbol, atau perforasi yang memiliki makna atau dapat dipahami oleh orang yang mampu membaca atau memahaminya.

Money Laundering Act (2002)	Combating Terrorism Act (2003)	Human Trafficking Act (2007)
Article 1 (7) Documents are data, records, or information that can be seen, read and/or heard, which can be issued with or without the help of an instrument, whether on paper, physical objects other than paper, or electronically, including but not limited to: a. writing, sound, or image; b. map, plan, photograph, or the like; c. letters, signs, numbers, symbols, or perforations having meaning or can be understood by people who are able to read or understand. Article 38 Examination of evidence in the form of money laundering: a. evidence referred to in the Code of Criminal Procedure; b. other evidence in the form of spoken information, sent, received, or stored electronically by means of an optical or similar to it, and c. documents referred to in Article 1 paragraph 7.	Article 27 Examination of evidence in criminal acts of terrorism include: a. evidence referred to in the Code of Criminal Procedure; b. other evidence in the form of spoken information, sent, received, or stored electronically by means of an optical or similar to it, and c. data, records, or information that can be seen, read and/or heard, which can be issued with or without the help of an instrument, whether on paper, physical objects other than paper, or electronically, including but not limited to: 1) writing, sound, or image; 2) a map, plan, photograph, or the like; 3) letters, signs, numbers, symbols, or perforations having meaning or can be understood by people who are able to read or understand.	Article 29 Evidence other than as specified in the Code of Criminal Procedure, may also be: a. spoken information, sent, received, or stored electronically by means of an optical or similar to it, and b. data, records, or information that can be seen, read and/or heard, which can be issued with or without the help of an instrument, whether on paper, any physical object other than paper, or electronically, including without limitation to: 1) writing, sound, or image; 2) a map, plan, photograph, or the like, or 3) letters, signs, numbers, symbols, or perforations having meaning or can be understood by people who are able to read or understand.

After the enactment of the EIT Law, the dualism of electronic evidence should have been clearly solved, because it was explicitly stated in article 5 that electronic evidence should be classified as legal evidence, as follows:

(1) Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah.

(2) Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya sebagaimana dimaksud pada ayat (1) merupakan perluasan dari alat bukti yang sah sesuai dengan Hukum Acara yang berlaku di Indonesia.

(3) Informasi Elektronik dan/atau Dokumen Elektronik dinyatakan sah apabila menggunakan Sistem Elektronik sesuai dengan ketentuan yang diatur dalam Undang-Undang ini.

(4) Ketentuan mengenai Informasi Elektronik dan/atau Dokumen Elektronik sebagaimana dimaksud pada ayat (1) tidak berlaku untuk:

a. surat yang menurut Undang-Undang harus dibuat dalam bentuk tertulis; dan

b. surat beserta dokumennya yang menurut Undang-Undang harus dibuat dalam bentuk akta notaril atau akta yang dibuat oleh pejabat pembuat akta.

1) Electronic information and/or electronic document and/or its print-out constitute a token of evidence which is legitimate and has legitimate legal effect.

(2) The electronic information and/or electronic document and/or its print-out as referred to in paragraph (1) constitutes expansion of legitimate token of evidence pursuant to the Law of Procedure prevailing in Indonesia.

(3) The electronic information and/or electronic document will be declared legitimate when it uses the electronic system pursuant to statutory of this Act.

(4) The provisions on the electronic information and/or document as referred to in paragraph (1) shall not apply to:

a. mails which under the laws shall be prepared in the written form;

b. mails and its documents which under the

prevailing statutory regulation require legalization by notary public or competent authorities.

The provisions of article 5 could be acknowledged as the extensive interpretation of existing legal evidence, or it could be categorized as a new order of legal evidence. However, for many, it is the consequences of the reliability of electronic evidence that in turn influences the degree of authenticity of the evidence (probative value) that is important. This is consistent with the terms set out in article 9 of the UNCITRAL Model Law on Electronic Commerce for accommodating the legal value of an electronic record by implementing the functional equivalent approach to the implementation of the security principles as a mechanism to determine reliability and trustworthiness.[5]

The differences between criminal proceedings and civil proceedings

As with other jurisdictions, there are differences in the principles of proof between criminal procedural law and civil procedural law in Indonesia. There is a difference in Indonesian criminal procedural law, in that there are two processes in the investigation, namely the (i) the preliminary investigation in order to gather information about the case (*penyelidikan*), and (ii) the legal investigation in order to find the culprit (*penyidikan*). The relevant evidence is distinguished by object evidence (*barang bukti*) and legal evidence (*alat bukti*). Object evidence is anything that is used as a result of the criminal activity, while legal evidence (for example an official letter, witness, experts statement, directive/information, statement of defendant) is a form of legal tool for proof that could be used to convey clear information from the investigation.

Article 43(2) of the EIT law has similar provisions to article 15 of the Convention on Cybercrime[6] concerning the safeguards:

> Penyidikan di bidang Teknologi Informasi dan Transaksi Elektronik sebagaimana dimaksud pada ayat (1) dilakukan dengan memperhatikan perlindungan terhadap privasi, kerahasiaan, kelancaran layanan publik, integritas data, atau keutuhan data sesuai dengan ketentuan Peraturan Perundang-undangan.
>
> Investigation on information technology and electronic transaction as referred to in paragraph (1) shall be conducted with respect to the protection of privacy, confidentiality, smooth public service, data integrity, or the integrity of the data in accordance with the provisions of legislation.

In addition, article 43(8) of the EIT Law provides that the investigator has the power to cooperate with other countries, and to request Mutual Legal Assistance:[7]

> Dalam rangka mengungkap tindak pidana Informasi Elektronik dan Transaksi Elektronik, penyidik dapat berkerja sama dengan penyidik negara lain untuk berbagi informasi dan alat bukti.
>
> In order to uncover the crimes of electronic information and electronic transactions, investigators can work together with other state investigators to share information and evidence.

Electronic evidence, electronic signatures and probative value

Five types of the legal evidence are recognized under article 184 of the Criminal Procedures Code: (a) the witness, (b) statements of experts, (c) a letter, (d) directive,[8] and (e) a statement of the defendant. Article 164 HIR also recognizes that there are five types of evidence, namely (a) the written evidence, (b) evidence of the witnesses, (c) presumption/inference, (d) confession and (5) the oath. There is a problem, because there is no explicit mention of electronic words or terminology, which has resulted in a difference of opinion between legal scholars on how to accommodate electronic evidence in a

5 *Two issues arose in discussion in the House of Parliament over the discussion of the formulation of article 5: whether electronic evidence may be considered as an extension of the evidence generally, or if electronic evidence can stand alone if it meets the applicable provisions of the Act. As one of the people that wrote the Act, the author indicated that it would depend on the context and the technical characteristics inherent in the electronic information itself, and will also depend on the scope of the law.*

6 *Budapest, 23.XI.2001.*

7 *There is also a specific law, Indonesian Law No 1 of 2006 concerning Mutual Legal Assistance that acknowledges and accommodates an electronic document as legal evidence, and also can be exchanged or communicated through the electronic system by investigators.*

8 *Directive or judicial notice is legal evidence that came from the correlated information from other related legal evidence, stated from witness statement, letters or testimony. (Article 188 Criminal Procedural Code: (1) Directive is an act, event or condition, which is due to the correspondence, both from each other, as well as the crime itself, indicate that a crime has occurred and who was responsible; (2) The instructions referred to in subsection (1) may only be obtained from: (a). statements of witnesses; (b). letters; (c). testimony of the defendant; (3) Assessment of the strength of evidence of a clue in any particular state is done by the judge wisely consideration again after he held a full examination of the accuracy and precision based on his conscience.*

legal proceedings or the procedural law in Indonesia.[9]

In the context of criminal procedure, some scholars claim that the existence of evidence in the Criminal Procedure Code is very limited; they think there is no other evidence except such evidence that is already provided for in the Criminal Procedural Code. While other scholars have a different view, based on the text of the Criminal Procedure Code. Examples of this are reflected in the following: article 185(7) of the Criminal Procedure Code, which recognizes the existence of the word 'additional evidence that other legitimate'; article 41 of the Criminal Procedure Code, which states that the definition of 'letter' includes telegram, telex and letters that contain a message, and article 187(d), which states that the existence of other letters can only be valid if it is linked with the contents of another evidentiary tool.

By carefully considering the formulation of article 41 of the Criminal Procedure Code, the substance of electronic information could be accepted as 'letter' evidence if the word was interpreted expansively. In summary, electronic information can be included in the scope of the existing categorization as a 'letter', but unfortunately in terms of practical perception, it must be in the printed format. The contents should be relevant or materially connected to the other letter as evidence. It would have also been seen as corroborating evidence by the testimony of forensic experts who examined the validity or authenticity of electronic evidence in their professional statement. What a digital evidence specialist can declare in writing may be presented as the letters, while what is described can be declared in their testimony.

Before the Electronic Transactions law, the judicial practice about accepting electronic evidence differed, because judges have the right to freely choose to determine whether to consider electronic information as valid legal evidence. Invalid evidence was not binding on the judge. After the EIT Law, a judge cannot refuse or deny electronic evidence, merely because of doubts relating to the validity of the evidence.

Electronic evidence can be categorized into two kinds, namely: (i) information in electronic format that naturally explains the legal events as the recorded fact in the electronic media (a photograph), and (ii) electronic information that can explain more than just the legal events, in which the content can describe activities that have taken place, such as surveillance.[10] Complementary to the substantial differences, there is a critical question relating to the authenticity of the data.

The evidential value of electronic data depends on the authenticity, and therefore the reliability of the data. The trustworthiness of the information or the validity of an electronic document will be determined by the level of security of the system. If the electronic evidence can be considered to be authentic, the output is assumed to be valid evidence. For this reason, judges should examine the reliability of electronic information by exploring the trustworthiness of the evidence, taking into account the tests evolved by Mason (footnotes excluded):[11]

> '1. The data (both the content and associated metadata) that a party rely upon have not changed (or if the data have changed, there is an accurate and reliable method of recording the changes, including the reasons for any such changes) from the moment they were created to the moment they were submitted as evidence.
>
> 2. As a corollary to (1) above, it is necessary to demonstrate a continuity of the data not being altered between the moment the data were obtained for legal purposes and their submission as an exhibit.
>
> 3. As a corollary to (2) above, it should be possible to test any techniques that were used to obtain and process the data.
>
> 4. The data can be proven to be from the purported source.
>
> 5. The technical and organisational evidence demonstrates the integrity of the data is trustworthy, and is therefore considered to be reliable.'

9 *See HukumOnline, the Indonesian online legal news, ' Rekaman Elektronik Sebagai Alat Bukti Kembali Diperdebatkan' , 24 December 2009, (Electronic Recordings As Evidence becomes Debated Back), available at http://www.hukumonline.com/berita/baca/lt4b336c3540de3/rekaman-elektronik-sebagai-alat-bukti-kembali-diperdebatkan. According to Andi Hamzah (Chairman of the Criminal Procedure Bill Drafting Team), the electronic recording cannot be used as information evidence. Referring to article 188 paragraph (2) of the Criminal Procedure Code, the information evidence can only be obtained through witness statements, letters, and testimony of the defendant. ' There is not valid evidence yet, because still in an electronics,' he said. But there is a provision in the Bill of the revision of the Criminal Procedural Code that has not passed yet, according to which electronic records can be used as information evidence. Andi Hamzah explained that it is for the judge to assess the strength of the evidence. To that end, the judges need to be more careful and cautious in making judgments.*

10 *For a more detailed analysis, see Stephen Mason, gen ed, Electronic Evidence (3rd edn, LexisNexis Butterworths, 2012), 4.01.*

11 *Stephen Mason, gen ed, Electronic Evidence, 4.21, cited in full with permission from the author.*

The trustworthiness or the accountability of the evidence is regulated by article 15 of the EIT Law:

> (1) Setiap Penyelenggara Sistem Elektronik harus menyelenggarakan Sistem Elektronik secara andal dan aman serta bertanggung jawab terhadap beroperasinya Sistem Elektronik sebagaimana mestinya.
>
> (2) Penyelenggara Sistem Elektronik bertanggung jawab terhadap Penyelenggaraan Sistem Elektroniknya.
>
> (3) Ketentuan sebagaimana dimaksud pada ayat (2) tidak berlaku dalam hal dapat dibuktikan terjadinya keadaan memaksa, kesalahan, dan/atau kelalaian pihak pengguna Sistem Elektronik.
>
> (1) Each Coordinator must maintain Electronic Systems reliably and safely and be responsible for the operation of Electronic Systems as appropriate.
>
> (2) The maintainer of Electronic Systems is responsible for the Maintenance of Electronic Systems.
>
> (3) The provisions referred to in paragraph (2) do not apply in the case of the occurrence of proven compelling circumstances, the offense, and/or negligence on the part of consumers of Electronic Systems.

Article 6 of the EIT Law sets out the minimum requirement regarding the implementation of the functional equivalent approach pursuant to modification of the provisions of the UNCITRAL Model Law on Electronic Commerce:

> Dalam hal terdapat ketentuan lain selain yang diatur dalam Pasal 5 ayat (4) yang mensyaratkan bahwa suatu informasi harus berbentuk tertulis atau asli, Informasi Elektronik dan/atau Dokumen Elektronik dianggap sah sepanjang informasi yang tercantum di dalamnya dapat diakses, ditampilkan, dijamin keutuhannya, dan dapat dipertanggungjawabkan sehingga menerangkan suatu keadaan.
>
> In the event of any other rule than set out in Article 5 paragraph (4) which requires that the information must be written or original form, Electronic Information and/or Electronic Documents will be considered legitimate insofar as the totality of information contained therein can be guaranteed, accessed, presented and accounted for, so as to explain a condition.

In general, there are three types of electronic data in Indonesia (i) electronic data that does not include a security system (data with no digital signature or electronic authentication); (ii) data that is created from a system that has some form of security that is not accredited (such as messages with a digital signature from a certification authority outside Indonesia), and (iii) data that is created from a security system or supported by a certificate authority that has been accredited.

The promulgation of the EIT Law and government Regulation No. 82 of 2012 concerning Electronic Transactions and Implementation System (PP-PSTE), provided guidance for judges to assess the reliability of electronic systems. Under the Regulations, a certificate for trustworthiness is provided for private contractual services, although accreditation is voluntary. The highest level of authentication is from the national accredited providers, including the use of a digital signature, which is supported by an accredited certification authority that has a root certificate to the government certification authority or the National root certification authority.[12]

Electronic evidence in civil proceedings

In the context of civil proceedings, article 1866 of the Civil Code and article 164 HIR recognize the existence of the following: (i) written evidence, (ii) the witnesses, (iii) presumption/inference, (iv) confession and (v) the oath. There are two types of written evidence, namely (i) a private deed made by the parties, and (ii) an authentic deed, which is made by public officials (article 1867 KUHPer). The second type of deed has the most strength value of evidence.

An authentic deed is a deed that has been drawn up in a legal format, by or before public officials who are authorized to do so at the location where this takes place. There is a legal presumption, due to the formal procedures that are implemented by the notary, that the substantial or material part of the deed has been achieved.[13] An authentic deed provides the best or conclusive evidence regarding the contents. However, an authentic deed does not provide conclusive evidence in respect of any kind of description, unless the information contained therein is connected directly with the subject of the deed. If the information described is not directly connected with the subject of the deed, this only serves as initial written evidence (article 1870).

It should be noted that an authentic deed cannot be treated as authentic deed if an official does not draw it up

12 *Article 61, Regulation No. 82 of 2012 concerning the Electronic System and Transaction Implementation.*

13 *Law No. 30 of 2004 concerning Jabatan Notaris (Public Notary) provides that the authentic deed is considered as the best evidence because it contains formal and material truth.*

with legal capacity, or because of a defect in form. In such circumstances, it only has the strength of evidence as a private deed if the parties sign the deed. In other words, due to the incompetence or incapability of the notary, or due to the absence of format, it cannot be regarded as an authentic deed, although it could be enforced as a private deed if the parties execute the document (article 1869 KUHPer). In the event that any type of authentic deed is found to be forged, then the execution is cancelled in accordance with the legal regulations of the Civil Legal Procedure/HIR (article 1872 KUHPer). The agreements concluded pursuant to a separate deed, such as the breach of the original, only provide limited evidence among the parties to such a deed, and it does not apply to third parties (article 1873 KUHPer).

Private deeds comprise all privately signed deeds, letters, registers, documents pertaining to household matters and other documents, which are drawn up without the intervention of a public official. A finger-print is the equivalent of a signature on a private document, certified by a dated and signed statement of a public notary or another official designated by ordinance, which stipulates that he knows the party affixing the finger-print, or that this party has been made known to him, that the contents of the deed have been explained to the party affixing the finger-print, and that, thereafter, the finger-print has been affixed in the presence of the official. The official shall record the document. Pursuant to further regulations, further rules may be stipulated regarding the statement and recording as abovementioned (article 1874 KUHPer).

If the interested parties so desire, executed private documents may be provided with a dated and signed statement of a notary or another official designated by ordinance, in which it is stated that he knows the signatory, or that he has been introduced to him, that the contents of the deed have been explained to the signatory, and that thereafter, the signing took place in the presence of the official. The stipulation in the third and fourth paragraphs of the previous article shall apply in this regard (article 1874a KUHPer).

A private deed, which has been acknowledged as the truth by the individual to whom it may refer, or which shall be considered legally acknowledged as the truth, is required to provide, with respect to the signatories and their heirs and parties having rights therein, conclusive evidence similar as an authentic deed, and the stipulation in article 1871 is applicable in this regard (article 1875).

An individual whose private deed has been disputed, is required to acknowledge or deny that such is his handwriting or signature; however is it sufficient for his heirs or parties having rights therein to declare that they do not recognize the handwriting or the signature as the handwriting and signature of the individual that they represent (article 1876 KUHPer). In the event that a party denies the writing or signature as his, or even if the heirs and the rightful parties declare that they do not recognize the writing or signatory, the judge must require the authenticity of the document to be investigated (article 1877 KUHPer).

From the above mentioned, at least in the context of civil procedure, there are three possibilities that can occur, namely: (i) the validity of electronic evidence acknowledged by the parties even though the electronic system was not accredited; (ii) the validity of electronic evidence that is not acknowledged by one of the parties that will dismiss or deny the truth in a trial, and the electronic system is not credited, and (iii) the validity of electronic evidence that could not be dismissed or denied by any of the parties, because the electronic system has been acccredited. The validity or reliablity of the electronic evidence cannot be denied because the systems had been audited, certified or accredited, unless the party that challenges the authenticity of the evidence can show that the system cannot be trusted.

In the first variant, the electronic evidence could be classified as private deed, but in practice it is similar with the authentic deed because the parties accept the evidence and do not deny its existence. With the second variant, where an opposing party challenges the authenticity of the electronic evidence, the judge will be required to decide the validity of the evidence with the help of a digital evidence specialist. Based on the inspection, if the digital evidence specialist considers that the evidence is original or authentic, then it will be treated as valid evidence, and the opposing party is no longer able to deny the admission of the evidence in the proceedings. The defendant will pay the cost of this exercise.

While the third variant, as befits an authentic deed, the judge can directly accept it as credible evidence because of the presence of a security system properly maintained (audited, certified or accredited), and the authenticity of the material has the value of full proof, unless the party challenging the evidence can prove that it does not meet the authentic deed formalities properly.

Probative value

At the lowest level, electronic information is objectively not assured unless external factors demonstrate that it is authentic. However, electronic data should not be denied simply because of its existence in electronic form,

so that a judge can consider the 'functional equivalence' principles in accepting the evidence as if it was written, original and signed.

In the intermediate level, if electronic information can objectively meet one of the several elements in a secured communication, then it is capable of being considered to be more valid. A third party might be able to objectively guarantee its validity, but there is still an opportunity to repudiate. That will probably be because the electronic system does not use a trusted third party to support the existence of electronic evidence. If there is no accountability or reliability of electronic systems, it means there is no guarantee that the system would be working properly. The electronic system does not have to accredited, but the opposition party can easily challenge it.

At the highest level, electronic information is objectively assured in its validity by being able to demonstrate the persons who are responsible for the document as well as assurance of the electronic systems were working properly. In this situation, the electronic system is accredited, so that unless the parties prove otherwise, then what is expressed by the system can be presumed technically and legally valid. In this context, the electronic information can be considered to have been properly maintained and the material or substance of the data should be treated as equal as or at least similar with an authentic deed.

The attribution principles of the electronic information that was exchange through the electronic system will be as appropriate as the security system itself. There is a presumption of the attribution of what the electronic information or electronic document should be. The procedural law is required to look at the general principles of the attribution of electronic records by considering the characteristics of the security mechanisms in the communication system.

Furthermore, a digital signature requires supporting information from an electronic certificate that supports its existence for it to have an evidential purpose. It is almost similar to the conventional signature that was attached to the paper National Identity Card issued by the government that could be classified as an authentic deed. The official signature affixed on the deed has a similar function to a public key to verify the signature. Without using a trusted third party, there is always an opportunity to deny or to repudiate the signature. Therefore to reduce the risk of repudiation (not to eliminate the risk), it would be more effective to use a trusted third party, such as a notary public, who can help to attest the use of electronic signatures in the transaction (cybernotary). In other words, the cybernotary could be used to support the validity of electronic evidence for the parties.

The cybernotary or electronic notary can certainly reduce the potential fraud in electronic transactions, and the notary with their electronic system applications can also help to provide for the validity of electronic evidence. The notary also has an opportunity to play a significant role and function to guarantee the authenticity of private and public documents. They can also help the Certification Service Provider or Certification Authority (CA) by providing a supporting function as the Registration Authority, or they can provide the services as a sub-CA. In short, the digital signature could be treated as the best evidence or having the strongest probative value, supported as it is by an electronic certificate involving the notary in their services and rooted to the government public key infrastructure.

Conclusion

The evidentiary value of electronic data as digital evidence is strongly associated with the reliability of the process and mechanisms of the security system. Less security might mean the weakest probative value. The weakest probative value is digital evidence that does not use security systems, which means there is no assurance about the integrity of the data. The legal consequence is that a judge is free to accept or to refuse such evidence as the best evidence, although the functional equivalent approach remains possible to implement.

The intermediate probative value is where digital evidence uses a security system, but is not certified or accredited. The opposing parties still has an opportunity to dismiss or to repudiate it as the best evidence. Including in the scope of this intermediate value are digital signatures from foreign countries, but which are not accredited in Indonesia. The strongest probative value is digital evidence that uses certified and accredited security systems which were supported by notary public or use the root system of the government PKI or the National Root CA.

Dr Edmon Makarim, S.Kom., S.H., LL.M., is a lecturer and researcher in Cyber Law (Telematics Law) and Intellectual Property Rights at the Faculty of Law, University of Indonesia, and a senior researcher at the Legal Research Institute for Technology Law, Lembaga Kajian Hukum dan Teknologi FHUI.

http://staff.ui.ac.id/edmon

edmon@ui.ac.id

edmon_makarim@yahoo.com