

Association for Information Systems

## AIS Electronic Library (AISeL)

---

ICEB 2003 Proceedings

International Conference on Electronic Business  
(ICEB)

---

Winter 12-9-2003

### Legal Protection for the E-Commerce in Indonesia: A Study on the Development and the Future of Cyberlaw in Indonesian Legal System

Sonny Zulhuda

Follow this and additional works at: <https://aisel.aisnet.org/iceb2003>

---

This material is brought to you by the International Conference on Electronic Business (ICEB) at AIS Electronic Library (AISeL). It has been accepted for inclusion in ICEB 2003 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact [elibrary@aisnet.org](mailto:elibrary@aisnet.org).

# Legal Protection for the E-Commerce in Indonesia: A Study on the Development and the Future of Cyberlaw in Indonesian Legal System

Sonny Zulhuda

Center for Regulatory Research  
Jakarta – Indonesia  
[zulhuda@yahoo.com](mailto:zulhuda@yahoo.com)

## Abstract

In this new economy, electronic commerce has paved its way for every business stakeholders, be it merchants, investors, distributors and consumers. Putting their contribution this way, they are understandably eager to see the road they are taking is safely guaranteed to deliver the aimed result. Due to this, efforts and strategies are being assessed, planned, undertaken and evaluated to mitigate and manage the risks associated with e-commerce, most notably from legal and regulatory approaches.

The thrust of this paper is to analyze current situation of e-commerce in Indonesia from the legal point of view. It will examine the problems that have accrued so far in the lacuna of a comprehensive cyberlaw in the country based on local incidents and cases. Special analysis will be given on main provisions of the Electronic Information and Transaction Bill to see how much protection it would give to the e-commerce activities in Indonesia and which parts should be better improved. At the end, the paper tries to summarize overall development and future of cyberlaw and its prospect of facilitating the growth of e-commerce in Indonesia.

This study serves to compliment as comparison for other assessments of the growth of e-commerce globally and regionally. Looking at the fact that Indonesia is just another crucial market power in this region, the study of its legal system in the e-commerce is both imminent and unavoidable.

## 1. Introduction

In this new economy, electronic commerce has paved its way to become another 'new kid on the block' where more investors are putting their shares and more players are taking their parts. Not only this phenomenon is imminent in the developed economies, but also it is witnessed in the developing countries. It is the consequence of this intensified situation that more stakeholders want to see the road they are taking is safely guaranteed to deliver the aimed result. Due to this, more efforts are now undertaken to mitigate and manage the

risks associated with e-commerce, most notably from legal and regulatory approaches.

Nevertheless, before moving further to defining the nature that the e-commerce has, and the risks it comes along, one would need to take a look back on how this new dimension of economy manages to get its place in most of the countries on this globe. In as much as the e-commerce begins to reshape the developed country's economy, it also takes its way in the developing countries.

E-commerce has certainly allured developing countries mainly due to several characteristics it has to offer. First, as Minges [11] indicates, it certainly increases the sales and thus generates hard currency. In other word, subject to different level of success indifferent places and situations, the e-commerce proves to be workable. This fact will in turn boost employment and welfare, and apparently has some effect on reducing brain drain and urbanization alike.

What attracts business players most is the unprecedented level of transparency and efficiency that is offered by e-commerce, especially in the infant democracies such as found in the developing countries. These factors of transparency and efficiency have apparently rejuvenated business players in conducting their course of business. Taken together, all these factors provide explanation on the emerging role given to the e-commerce sector in reshaping the new economy in many developing countries.

## 2. E-commerce in Indonesia

### 2.1 Facts and Figures

Indonesia is the largest archipelago country in the world with more than 16,700 islands, spreading across 5,000 km of equatorial line. With a population of more than 210 million (Source: Indonesia Bureau of Statistics at [www.bps.go.id](http://www.bps.go.id)), Indonesia is the 4th most populous country in the world. Although the country covers a large area, the population is concentrated in the islands of Java, Bali and Sumatra.

Like many other countries in Asian region, Indonesia also felt the effects of the economic crisis, which prevailed globally since 1997. That crisis hit Indonesian economy very badly. Data show that since 1997, GDP (gross domestic product) and income per capita have been decreasing [17]. But those numbers were improved in 1999 onwards because of the Indonesian economy recovery program under the new government.

Indonesia's demographic and geographic situation would appear to make it an ideal location for e-commerce. There is a large market spread over many islands. However, the current reality does not really reflect the expected impact. Indonesian 'e-readiness' – shorthand for the extent to which a country's business environment is conducive to Internet-based commercial opportunities– trails behind other developing countries in the region. The e-readiness ranking in 2002 placed Indonesia 52<sup>nd</sup>; trailing behind Singapore (11<sup>th</sup>), Malaysia (32<sup>nd</sup>), Thailand (46<sup>th</sup>) and the Philippines (49<sup>th</sup>), and only ahead of Vietnam (56<sup>th</sup>) [16].

The Indonesian Association of Internet Service Providers (APJII) [1] stipulates that the number of Internet users in Indonesia is 4.5 million in year 2002 (2.14% of the population), and at the end of 2003 is estimated at 7.550 million (about 3.5%). Refreshingly, until March 2003, the number of ISP that has been issued license reached 186 (See Table 1).

**Table 1: Internet and e-commerce indicators in Indonesia. Source: Association of Internet Service Providers Indonesia ([www.apjii.or.id](http://www.apjii.or.id))**

	1999	2003 (till 1st quarter)
<b>Internet Users</b>	1,000,000	7,550,000
<b>Internet Subscribers</b>	256,000	800,000
<b>Internet Service Providers</b>	50	186
<b>Country top level domain (.id)</b>	3627	16,257

A survey performed by US-based Boston Consulting Group (BCG) of 14 Asian countries found that Indonesia's per-capita online spending was \$0.01 in 1999 (or a total of \$2m), leaving it behind India (\$0.03), Thailand (\$0.02) and Malaysia (\$0.05). BCG said 80% of the online transactions in Indonesia came via travel-related websites [3].

By volume, the accumulated value of e-commerce in Indonesia has been estimated at under US\$ 100 million in 2000, or less than 0.1 per cent of GDP [8] and only represents 0.026% of the total world transaction value that reached USD 390 billion in the same period [17].

Despite those discouraging figures, the future of e-business is still shining in Indonesia, provided that the existing barrier can be handled well. The hope can well emerge from the fact that Indonesia appears to be the freest Internet market in Indonesia. This is a direct impact of an unprecedented liberalization and freedom to speech unleashed by the current open political environment [8]. There are at present no limits on the number of Internet providers nor is content restricted in anyway.

According to recent statistics of Indonesian Association of Internet Service Providers (ISP), there is significant growth in all Internet-related figures: number of Internet users, Internet subscribers, Country Top Level Domain (CTLD), and number of ISP's in the last five years [1].

International Data Corp, a US research firm, estimated that the number of Indonesians who buy goods via the Internet would swell to 600,000 by 2003 (from 70,000 in 2000). It counted 3,544 websites managed by Indonesian companies, with upwards of 50 being Internet service providers [3].

## 2.2 E-commerce Barrier

Given the ideal expectation for the e-commerce in Indonesia, question may now be posed as to why e-commerce does not make a real big jump in Indonesia. This is purportedly due to existence of several barriers to e-commerce development, including lack of infrastructure (of both technological and regulatory), awareness, security, etc.

This paper foresees that legal, regulatory and policy frameworks count as among the major force to facilitate e-commerce development. For this reason also, this aspect has been made integral to the concept of e-readiness.

It is this importance that has been emphasized by the government of Indonesia when developing and formulating the national information system or called SISFONAS [15]. By virtue of this platform, the government of Indonesia shares the vision that there shall be an '*i before e*', or, infrastructure before going electronic. And this infrastructure includes regulation.

Looking at this fact, the fate of e-business certainly hinges on the adequacy of legal and regulatory frameworks that should serve as rule of the game. Inadequacy and lack of enforcement thus serve as detrimental barrier for the development of e-commerce.

The issues such as consumer protection, formation and delivery of contract, payment method, transaction security and data confidentiality have become a main menu when consumers consider e-business transaction.

The questions remains are to what extent all the stakeholders, mainly the authorities, have anticipated the legal and regulatory aspect of e-commerce.

### **3. Legal Protection for E-commerce in Indonesia**

#### **3.1 Current State of E-Business Law in Indonesia**

In Indonesia, demand to upgrade the protection of laws for e-commerce environment is arising [5]. Steps have been initiated but considered very slow. While other countries in the region have had some pieces of legislation in place, there is no single act comprehensively addresses the issues of cyberlaw.

The main law currently deals with telecommunications sector is the Telecommunication Law No. 36/1999 [8]. However, this law mainly deals with the broad telecommunication sector, licenses, operation, network provision, and other procedural matters. It does not touch issues of content and other aspects of cyberlaws.

Despite the absence of a comprehensive cyberlaw, some redresses have been attempted from the existing traditional laws such as in online credit card fraud cases. But in many occasions it is proved that these laws are just not sufficient enough to accommodate special nature and challenges of e-commerce age. The penalties stipulated for cyber crime offenders often do not sufficiently bring about the deterrent effect, and existing punishment does not necessarily remedy the loss that may accrue.

Currently, Indonesia's Central Bank (Bank Indonesia or BI) is taking initiative to prepare draft law on fund transfer act. The law among other things will touch the issue of electronic transfer of fund between financial and banking institutions [2]. However, it submitted that the process that this draft will take to become law will still be long.

At administrative level, there is however a good signal from the Government when recently Presidential Decree No. 3/2003 was issued namely 'National Policy and Strategy on E-Government' in June 2003 [1]. The decree basically urges all sectors of government agencies in central and provincial levels to prepare and accommodate infrastructures, methods, procedures and human resources for the implementation of e-government. With this decree, the government is apparently ready to embark further with online environment of governance including official e-procurements.

To this extent, it can be summed up that the current state of e-business law in Indonesia is in its initial stage. Some scattered and conventional laws are still in use for cyberspace medium with limitations, while the government has taken some administrative measures to

embark themselves into online environment through the implementation of e-government.

On the top of this, it is worthy to note that this lacuna would be answered quite soon by the initiative to legislate a comprehensive cyberlaw legislation to be elaborated later in this paper. But first we would need to see some legal challenges that have been faced by e-business in Indonesia.

#### **3.2 Challenges to Indonesia's E-business Law**

The initial process of e-commerce in Indonesia that is discussed earlier may account partly for the present rudimentary state of Indonesian laws on electronic commerce. This condition, however, can also be seen as a reflection of the current state of the development of Indonesian business laws in general [6].

It is true in the sense that Indonesia still relies heavily on laws and regulations that are issued during the Dutch colonial rule to regulate such fundamental matters as contracts and evidence. This situation requires reform, which cannot accomplish overnight.

The urgency for legal reform in e-business area is furthermore warranted by rampant cases of infringement and violation of laws that relate to the e-commerce activities. Among those incidences are described in the following passages.

##### **3.2.1 Online Copyright Infringement**

The Ministry of Justice is responsible for Intellectual Property Rights. As far as copyright law is concerned, Indonesia has a copyright law and is a signatory to the Berne Convention. In general, foreign copyrights receive automatic protection in Indonesia but there is lack of resources for enforcement.

Indonesia has been cited as having the third highest software piracy in the world, 89 per cent in 2000 that results in a loss of US\$ 70 million [8].

Certainly, poor level of protection for the intellectual property rights is not a good signal for potential investors and consumers to come into Indonesian market. The government had just recently enforced the new copyright law (Copyright Law 19/2002) that comes with effect of more severe penalty for the copyright infringement.

The law has also accommodated what it needs to meet the e-commerce challenges. It expressly includes the Internet as one of the publication medium in which a copyrighted material may also be infringed. The law has made equal protection for the copyright in the online media, and thus clearing the way for e-business to operate safely.

For effective enforcement, the law gives more power to the law enforcers in order to conduct search and seizure of suspected infringement. This law has given a blow to online piracy movement in Indonesia; nevertheless, the effective enforcement of it still remains for us to see.

### 3.2.2 Internet Credit Card Fraud

Internet fraud is fast becoming a common factor in online retailing as e-commerce transactions rise and fraudsters develop more sophisticated methods. According to Gartner G2 research, the risk of Internet payment fraud is at least 12 times higher than it is for face-to-face transactions.

Unfortunately, this online credit card fraud (widely labeled 'carding') has been so much associated with Indonesia. In year 2002 an international online fraud survey by *ClearCommerce* listed the country in the two top twelve countries from where the most online credit card fraud originates, only second to Ukraine (see [www.ocalasmostwanted.com](http://www.ocalasmostwanted.com)). It was suggested that about 20% of credit card transaction from Indonesia was suspected to be illegal.

In year 2002 alone, there were 218 cases of credit card fraud reported to the Police [9]. Meanwhile, there have been 23 cases reported in 2003 (until August). Out of these incidences, only a handful cases have been successfully handled by the Police.

The victim of this scam is worldwide. In 2002, most of the victims were American (84 cases), and following the US are mainly victims from developed countries in the Canada, Europe, Australia, and East Asia.

This rampant incidence costs Indonesian e-commerce at inconvenience. According to *Gatra Magazine* [8], online transaction requests that originate from Indonesia's IP addresses have been rejected and blocked.

In dealing with these cases, law enforcers have encountered certain legal obstacles. This is mainly the result of absence of a comprehensive cyberlaw that would otherwise anticipate cases like these. It was reported that the Police in this instance seek remedy from the conventional Penal Code with so many limitations, especially in defining the constitution of commission of crime and defining evidentiary issues.

As said earlier, these rampant abuses of the e-commerce activities in Indonesia have warranted the urgency of enacting a comprehensive cyberlaw in order to ensure reliability of e-business, as well as the confidence of consumers, merchants and investors to embark in the new venture.

## 4. Assessment of Indonesia's Cyberlaw Bill: Electronic Information and Transaction Bill

The current Electronic Information and Transaction Bill ('the Bill') [12] is considered the first initiative of the country to enact a comprehensive legislation on cyberlaw. There were initially two government's agencies that came out with two different bill drafts at the same time. This fact reserves some comment in the later part of this paper.

The Ministry of Industry and Trade initiated the draft of Electronic Information and Electronic Transaction Bill. On the other hand, the Department of Tourism, Post and Telecommunication under the Ministry of Transport also came out with the draft of Information Technology Bill. This double initiative was uncoordinated creating prolonged, unfocused and unnecessary debates among academics and IT professionals.

Nevertheless, the debates were deemed to have brought constructive ideas as well. It is noteworthy that the two drafts took different approach in formulating cyberlaw into legislation. While the Electronic Information and Electronic Transaction Bill was concentrated on e-commerce law and related aspects taking into account the requirements under UNCITRAL model law on e-commerce, the IT Bill was a general law (some called 'umbrella law') dealing with so many issues on general terms.

After some years of debates, the government acted wisely to coordinate and merge the efforts together. The coordinating agency is now Ministry of Communications and Information, and the consolidated draft is now called Electronic Information and Transaction Bill.

The approach is somehow a hybrid of the two original drafts; it does cover quite extensive subject matters from e-contract to e-signature, from privacy and personal data to cyber squatting and intellectual property rights, and from cyber crimes to consumer protection. However, the Bill does not go lengthy enough in subject matters other than cyber crime, e-contract and related aspects. For other subject matters, the Bill provides that they will be governed by subsidiary regulations.

At present, the draft Bill had been finalized by relevant agencies after it was consulted to public for comment. It was reported in June this year that the Ministry has processed the Bill to be signed by the President and ready to be tabled to Parliament [14]. It is presumed that the Bill will be enacted not later than the first quarter of year 2004.

Since this draft bill is the first to accommodate cyberlaw requirements, once enacted the law will certainly provide basis for the reform or revision of other areas of laws including electronic fund transfer, e-

government, capital market, online taxation, and online banking.

#### **4.1 Legal Position of Electronic Message & Admissibility of Electronic Evidence**

The Bill acknowledges in section 4 that electronic information shall have legal effect as evidence. This proposition includes the print-out form generated from the electronic message. However, for its legal effect, the electronic message is required to have generated from electronic system that is reliable. Furthermore it also stipulates that the electronic information system must fulfill requirements of integrity, reliability, and accessibility. It also has to be able to retrieve the message it is required. Having said this, however, the Bill stipulates that there are some exceptions in certain matters where written document is still necessary & essential including the marriage contract and land matter.

#### **4.2. Consumer Protection**

It is stipulated in the Bill that everyone has the right to obtain accurate and complete information with respect to contract requirements, manufacturer, and product that is offered electronically section 10(1). For this purpose there can be reliability certification body to be jointly worked out by government and members of public.

In respect with dispute resolution methods, consumers are given variety of legal redresses by the Bill. In case there is found *any use of IT* by certain party that creates harm for society, a class action can be taken by virtue of section 37. Arguably, this *'use of IT'* is wide enough to cover many areas and issues to the favor of consumers.

Besides, civil action can also be brought to commercial court in the event there is a use of IT that causes commercial loss to the consumers. In certain circumstances where there is a threat to certain important aspect of public life, the government may instead take action to protect public interest.

Other than litigation, consumers are also given option to settle their e-commerce disputes by employing alternative dispute resolution (ADR) including arbitration as provided in section 42, and the decision resulting from such process shall be final and binding upon the disputing parties.

#### **4.3 Electronic Contract**

The principle of freedom of contract is strongly upheld by the Bill when it stipulates the freedom of contracting parties as to which law to govern, and in which forum to hear the disputes. In this respect, alternative dispute resolution is also available for the contracting parties to opt.

More than expected, the Bill does not only recognize the legal effect of an electronic contract and parties to it, but also places the e-contract inline with the requirements of international civil law. This international civil law would be the reference in the event where contracting parties do not specifically stipulate which law would govern their agreement. This stipulation in section 20 (3) is especially important in the event dispute arises and the parties did not specify which law is to be the governing law.

The constitution of e-contract still depends on the offer and acceptance of the offer; nevertheless the principles are being adjusted to the online environment. Furthermore, by virtue of section 23(3) the use of electronic agent for a contract can also be held binding as far as the electronic agent is functioning properly in the ordinary course of business. This provision accommodates among other things the widely used Automatic Teller Machines (ATM) by banking industries. Other kinds of payment methods that involve automatic arrangement e.g. through computers are also covered under this provision.

Given the relatively new and ever-developing circumstances of the information technology, the Bill does anticipate its limitation in governing the e-contract activities. As a result, the Bill also provides in section 25 that any business customs and commercial practice those are alive today and not in contravention with the provisions of the Bill shall remain applicable.

#### **4.4 Writing & Signature Requirements**

Electronic message can be held original and shall fulfill the requirement of 'writing' provided that its integrity, reliability, accessibility, and retrievability are guaranteed.

Electronic signature has a valid legal effect under section 11, and the requirements are set in section 13. The word used is 'electronic' and not 'digital'. Meaning, it is technology neutral. And interestingly, it does not ever touch the technology of public key infrastructure. Meanwhile, the certification authority is not made compulsory; instead it was made optional (*'dapat'*) in section 15(1).

#### **4.5 Cyber Squatting**

Some aspects of domain name registration and related issues are touched in section 26 of the Bill. It recognizes any registration of domain names on first come first serve basis. However, this domain name shall not be registered under bad faith, should not trespass fair competition law, and should not infringe rights of others on the name.

If the latter occurs, the infringed party may take civil action for damages. While international system of registration is recognized, further procedure of names

registration would be regulated by subsidiary regulation. Arguably, this stipulation gives legal effect to the international arbitration procedures, e.g. those under WIPO, UDRP, etc.

#### **4.6 Intellectual Property Rights**

The Bill in section 27 recognizes and protects every intellectual property rights as the result of electronic information work, and same protection is given for Internet website design and any IP-righted materials it contains. This provision is very short and simple, purposely because there is already a comprehensive law deals with IP issues. Apparently the Bill tries to avoid overlapping with those IP legislations.

For instance, Indonesia's new copyright law No. 19/2002 does anticipate the information technology and what it may affect the copyrighted works. It already sufficiently provides that the same principles of copyright are applicable in the cyberspace medium.

#### **4.7 Personal Data Protection**

Personal data protection (PDP) has been among the most contentious issue in the cyberlaw discourse. This is due to many reasons, mainly its significance to two seemingly-contradictive things: human rights that demands maximum protection of privacy in one hand, and international trade that requires extensive personal data transfer on the other. This background leads to various international attempts to come with regulatory measures on PDP.

However, possibly to the surprise of many, the Bill only provides one section (section 28) to deal with PDP, and no subsidiary regulation is mandated by the draft.

It only stipulates that data subjects must give 'consent' before the 'use' of any information containing personal data and privacy rights of that party, except in relation to public information that are no longer confidential.

Questions arise as to whether there is similar protection in the event of collection, storage, or deletion of the same personal data? Also, what kind of 'consent' required? Is it an opt-in or opt-out model? Given the width of the issue, why very limited provisions in the Bill? And why no mandate is provided for any secondary legislation such as in other parts of the Bill?

#### **4.8 Offences of Cyber Crime**

The offences under proposed bill are among the most contentious issues. The first sight on Bill's provision suggests wide and extensive coverage of computer misuse types and categories.

First of all, it is Interesting to note that 'hacking' or a mere unauthorized access to a computer or electronic

system is not made an offence, in an opposite stand to the law in other major countries such as UK, Malaysia and Singapore. This is believed to be crucial since Indonesia has been known for its rampant cases on cyber crime involving hacking, web-defacing and credit card fraud.

Hacking is an offence only when, first, it is committed with the purpose of obtaining or altering information contained in that system. Secondly, it is committed with the intention to secure information classified as confidential, or that are detrimental for national security and international relations. It is argued that this provision on international relations and nation's critical information infrastructure would provide redress for the issues of cyber-terrorism.

Hacking is also an offence when it is committed against the electronic system of financial and banking industries, with the purpose of misusing it or gaining undue advantage out of it.

The Bill also criminalizes any action that posed harms to the proper functioning of nation's protected electronic system (e.g. those system under national critical infrastructures). 'Protected computer' is elaborated by the Bill's elucidation of section 34; to fall into two categories: first, special and exclusive computers that belong to the government's financial institutions, and secondly, the computers that are used by the state to communicate and trade with parties from other countries.

In other provision, the Bill makes it an offence for the wrongful communication of password, access code, or other means of access (section 35).

Credit card fraud is addressed in section 33, where it provides that, any way of unauthorized use or access of other people's credit card to gain benefit from e-commerce is an offence under the Bill. It is hoped that this provision may curb the existing problem and thus eliminate the notorious credit card fraud in Indonesia.

#### **4.9 Summary**

In this summary on our assessment on the Bill, there are some other aspects worth noting, including both advantages and weaknesses.

First appreciation worth to note is that draft has aptly acknowledged the nature of technology of the Internet and ICT that is ever changing, ever developing and very dynamic. Ready to face this nature, the draft expressly stipulates (in section 2) that the law to be enacted must be based on neutral technology basis.

This provision will enable the law to accommodate various and dynamic developments of the information and communication technology. All kinds of technology will be acknowledged and given legal effect as long as

the requirements of system integrity, reliability, and accessibility can be assured.

Since the cyberlaw is a *'lex specialis'* or special legislation, the drafts provides in section 3 another important provision, that any other existing laws that have some extent of ICT use and employment, will be deemed applicable. Thus, rather than repealing effect, the cyberlaws have instead acted as complimentary to other existing laws and regulation. This provision is very important to affect solid and comprehensive national legal system.

The Bill, however, reserves some considerations for improvement. The biggest limitation it posed may be associated to its wide but not-deep coverage, especially in the area of privacy and personal data protection.

Simple and short approach taken by the draft in dealing with other issues may also cause another inefficiencies of the law. The current draft Bill requires about eight regulations. Normally these regulations will take another time and process to achieve.

It appears that the civil procedures in the commercial court as provided by the Bill open room for delay of litigation. And this may create another factor of ineffectiveness of the law. By virtue of section 39, the court is given a maximum of 90 days from the date an action is registered to deliver judgment. An extension of 30 days is provided with the permission of Supreme Court. It submitted that a total of 120 days for the delivery of judgment is too a long period and may necessarily prejudice the action due to the nature of e-evidence that may be gone vary fast.

## 5. Final Remarks

The cyberlaw bill certainly is among the most long awaited legislation by anybody engaged in businesses in Indonesia. With e-commerce in Indonesia grows from time to time, legal and regulatory issues get more imminent and prevalent. It is very important that the current on-going process of the Bill's enactment be widely informed to all these business stakeholders.

While enacting the law is one remarkable achievement, attempts will need to be initiated to anticipate effective enforcement of the law itself. With the cyber crime cases getting more serious and rampant in Indonesia, the law once passed should be enforced as soon as possible.

To achieve maximum enforcement, at least three sectors need to be addressed. First, international and worldwide cooperation needs to be secured. This is due to the nature of cyber crime which is trans-border and extra-territorial. Certain kinds of collaboration needs to be initiated at region level first, and then to the global level.

Secondly, the Indonesian Government needs to ensure there are effective administrative measures, policies and strategies in executing the requirements of cyberlaw and e-government. The question such as which ministry or agency to take a lead will need to be answered to avoid overlapping tasks like what happened with the double draft bill on cyberlaw.

Last but not least, educational factor is urgent. Not only to create more Internet-literate society, but also to achieve most effective and efficient utilization of the ICT. It is foreseen that the problem of digital divide in the country is still an uphill task to solve. This is in anyway also to create more balanced and fairer digital society in the region.

With all these policies and strategies, the enactment of cyberlaw will serve its purpose especially in giving maximum protection for the future of e-commerce activities in Indonesia and the region.

## References

- [1] Asosiasi Penyelenggara Jasa Internet Indonesia (APJII). *Statistik APJII*, APJII homepage, URL at <http://www.apjii.org.id>.
- [2] "BI siapkan draf RUU transfer dana," *Kompas Online*, 17 February 2003, URL at <http://www.kompas.com>.
- [3] *Doing e-business in Indonesia*, URL at <http://www.ebusinessforum.com>.
- [4] "Enam pemuda bobol kartu kredit ditangkap," *Republika Online*, 17 July 2003, URL at <http://www.republika.co.id>.
- [5] Freddy Harris. "Menanti hukum di *cyberspace*," *Jurnal Hukum dan Teknologi*, 2001, vol. 1/1, 4-6.
- [6] Gingerich, D., & Christian Teo. *E-com legal guide: Indonesia*, January 2001, URL at <http://www.bakerinfo.com/apec/indoapec.htm>.
- [7] Hikmahanto Juwana. "Aspek penting pembentukan hukum teknologi informasi di Indonesia," *Jurnal Hukum Bisnis*, 2001, vol. 16 - November, 48-55.
- [8] International Telecommunication Union. *Kretek Internet: Indonesia case study*, March 2002, URL at <http://www.itu.int>.
- [9] "Menjepit ulah pembobol kartu kredit," *Gatra*, 43/IX, 13/09/2003, 26-35.
- [10] Mieke Komar Kantaatmadja (ed.). *Cyberlaw: suatu pengantar*, ELIPS II, Jakarta, 2002.
- [11] Minges, M. *E-commerce in three landlocked nations*, INET 2000, Developing Countries Networking Symposium, Yokohama-Japan, 2000
- [12] *Rancangan undang-undang Republik Indonesia tentang informasi dan transaksi elektronik*, Ministry of Communication and Information of the Republic of Indonesia, URL at <http://www.kominfo.go.id>.
- [13] Ridwan Khairandy. "Pembaruan hukum kontrak sebagai antisipasi transaksi electronic commerce," *Jurnal Hukum Bisnis*, 2001, vol. 16 - November, 56-64.
- [14] *RUU transaksi elektronik belum disampaikan ke DPR*, 27 June 2003, URL at <http://www.kominfo.go.id>.
- [15] *Sistem informasi nasional sebagai tulang punggung implementasi e-government*, Ministry of Communication and Information of the Republic of Indonesia, URL at <http://www.kominfo.go.id>.



[16] *The Economist Intelligence Unit e-readiness rankings*, July 2002. URL at <http://www.ebusinessforum.com>.

[17] Zuraida Boerhanoeddin. *E-commerce in Indonesia*, 2000, URL at [http://www.isoc.org/inet2000/cdproceedings/7c/7c\\_3.htm](http://www.isoc.org/inet2000/cdproceedings/7c/7c_3.htm)