hukum online.com
Issue 88, 28/3/2008

Indonesian
Weekly Law Digest

Indonesian Legal Digest *is a service of*
PT Justika Siar Publika *owner and operator of*
www.hukumonline.com
Puri Imperium Office Plaza UG 15
Kuningan, Jakarta 12319
to subscribe, call 62-21-83701827 or fax to 62-21 83701826
or email layanan@hukumonline.com

Bill on Information and Electronic Transactions - The DPR Approves

Overview

The House of Representatives (DPR) have finally been able to pass the Bill on Information and Electronic Transactions into what will become the prevailing law in this area (*Undang-undang Informasi dan Transaksi Elektronik* / UU ITE). The Bill first came before this DPR in September 2005 and this is the 96th bill to be passed into law by the DPR since 2004. It is worth pointing out that such a long gestation period is not uncommon for bills wanting to be passed into law. Unfortunately, it is not always the case of better late than never.

Much of the public commentary over the past few days has focused on Article 27(1) which prohibits the transmission, distribution, and the making available of material in an electronic form that breaches prevailing moral standards. However, the bill does not seem to criminalize those that choose to download this morally questionable material unless where once it is downloaded it is then transmitted to someone else.

However, the bill is about so much more than trying to limit the spread of what is considered to be morally suspect material. The bill deals with subject matter such as electronic signatures, electronic contracts, domain names, and electronic transactions. The overriding theme of the bill is to increase legal certainty and security for electronic transactions.

Much of the focus of the bill will not be on what it permits but rather on what it prohibits. In addition to the focus on pornography noted earlier the bill explicitly prohibits any electronic communication that threatens physical violence or strikes fear into the reader of the communication. The potential criminal liability for this is up to 12 years imprisonment and / or fines of up to IDR 2 billion.

Other prohibitions are expected such as the interception and tapping of communications and then the misuse or abuse of personal data. This would include such things as identity theft.

Table of Contents

Issue 88, 28/3/2008

The biggest question that the bill poses is enforcement; particularly where there conceivably are competing privacy rights. The bill is clear as to what is permitted and what is prohibited. Any internet user is aware of the great amount of anonymity in cyber space and myriad of web logs (blogs) are testament to this.

However, the bill would seem to grant the necessary powers and authorities to search and seize any tools or equipment allegedly used in the commission of an offence. Yet, it must be noted that the bill stipulates that investigators must comply with prevailing laws and regulations as they relate to privacy, confidentiality, the provision of public services, and the integrity of data. Therefore, this must be interpreted as preventing investigators from conducting fishing expeditions for example by requesting all the data of an internet service provider (ISP) in the hope of finding supporting evidence of a crime.

The definition of what constitutes evidence has been expanded beyond that of the provisions in current legislation to include specifically electronic information and electronic documents.

The Rationale for a Law on Information and Electronic Transactions

The world is a very different place than it was 5 years ago, 10 years ago, 20 years ago, or 50 years ago. We as a race of people are well and truly into the electronic age and much of our personal and professional existence relies on sophisticated technology. We can to all intents and purposes live online and never have to physically leave the places that we live, if we wanted to of course.

We can shop online for everything we need and do not need from groceries to books to pornography; we can work online; yes, just about everything we need to do is something that can be done online or electronically. Most of us if we thought about it would be able to identify an occasion where rather than get up out of our office chair and walk to a colleagues office we sent an email instead or an SMS in preference to calling and talking to a colleague or a friend. This in and of itself evidences how much of our lives are now dependent on technology.

We must therefore ask ourselves how safe are we in this virtual world? How safe are our identities? And, How safe are our transactions? If we do not ask ourselves these questions then we expose ourselves to considerable danger. For those that have never considered these issues the government has done so on your behalf and this bill is an attempt to provide regulatory certainty to information and electronic transactions that are conducted using the sophisticated technology now at our disposal.

The world has quickly become a borderless place in the sense that electronic transactions are instantaneous and cross traditional sovereign State lines without ever having to ask for directions or permission. This is in spite of some sovereign states trying to filter information and electronic transactions through selected and approved service providers. Most experts tend to agree that censorship and regulation in this way has often proved ineffective at best.

This phenomenon has given birth to cyber law and this bill fits within Indonesia's developing cyber law regulatory framework.

Scope of the Bill

A quick scan or reading of the 'General Provisions', which in an Indonesian law is usually where all the definitions of the terms are listed, highlights that the bill is about so much more than protecting Indonesians from themselves with respect to the perceived dangers of morally suspect behaviours such as pornography, gambling, and violence.

The definitions include entries for what constitutes an electronic transaction, what constitutes an electronic document, what constitutes an electronic agent, what constitutes an electronic certificate, what constitutes an electronic signature and the authentication and validity of any such signatures used in an electronic transaction, as well as who constitutes a sender and a receiver of an electronic document or piece of information.

Each of these definitions are important as this is a new area of law for most, including practitioners of the law who will ultimately be tasked with prosecuting or defending cases in this field along with the judges who will decide who is in breach of the provisions and who is not.

Article 2 purports to include a degree of extra-territoriality as it explicitly states that the provisions of this law apply to all persons who commit an act against the provisions of this law whether they are within the jurisdiction of the Republic of Indonesia or outside of it provided that the act committed is an offence either within the Republic of Indonesia or outside of it and it causes a loss to an Indonesian interest.

The Elucidation to the Law states that the utilization of information technology is trans-national and therefore universal, which thereby allows Indonesia's jurisdictional reach to extend beyond its physical borders and into the realm of cyber space.

It is likely that this extra-territorial jurisdiction that is proclaimed here is going to be heavily reliant on mutual legal assistance and bilateral extradition treaties.

The Point

The basic purpose of the bill is to:

- to develop a smarter nation able to participate more fully in the world of information;
- expand national trade and the national economy to improve the social welfare of the citizens;
- increase the levels of effective and efficient public services;
- provide broader and greater opportunities for citizens to develop their talents and skills; and
- to provide security, justice, and legal certainty to users and providers of information technology.

Information, Documents, and Electronic Signatures

The bill gets straight to the point in Article 5(1) in stating that electronic information, electronic documents, or any printed version of either is to be considered legally valid evidence. However, there are exceptions. In this case if there are certain documents that must be in written form or notarized, then an electronic version of these documents is presumably not acceptable evidence for the purposes of a criminal or civil hearing.

Interestingly, a business person who offers a product via an electronic system is obligated to provide all relevant information associated with the product being offered including any contract conditions, the producer of the product, and the product itself. Furthermore, these types of businesses must be certified by an accredited agency.

Electronic signatures are to be considered the same as any ordinary written signature and consequently binding at law provided it meets certain conditions. Generally, these conditions will require that evidence be adduced that the electronic signature at all relevant times was only under the control of the person who is alleged to be the owner of that signature.

In consideration of the binding nature of an electronic signature, the Law is explicit that any one who is involved in the use of electronic signatures is under a special duty of care to ensure the safety and security of the signature and the identity of the relevant person. Businesses and signature holders must pay particular note to this as Article 12(3) states unequivocally that any breach of the provisions relating to electronic signature exposes the person that causes the breach to be liable for all losses associated with the breach. This includes any legal consequences that arise in addition to the losses accrued.

Electronic Transactions

The critical feature of electronic transactions is that they can be either public or private but in any case they are binding on the parties who are signatories to them. An electronic transaction that binds the parties also allows those parties to choose the forum to resolve any disputes or grievances that may arise in the course of their contractual relationship. This includes court based mechanisms or arbitration or any other form of alternative dispute resolution. It must be noted that where one of the parties is international then the prevailing law is to be International Commercial Law.

Prohibitions

As was noted earlier much of the public debate and perhaps much private debate has centered more on what is prohibited under the provisions of the law as opposed to what is permitted. Furthermore, much of this debate has focused on the pornography components to the detriment of other critical prohibitions contained in the Law.

In terms of pornography the target of the legislation is clearly the disseminators, distributors, and transmitters of the offending material as opposed to the downloader of the suspect pictures. Nevertheless, businesses should be aware that for their own protection filters should be installed so that a legitimate claim to making an attempt to restrict access from office servers was made. It was pointed out earlier that historically software filters have been ineffective. This is not the point though.

It might prove for interesting legal argument if a company's internal server did not block offending material but allowed it to pass through to individual employee inboxes as to whether this would be a breach of the distributing or transmission provisions, particularly if the receiver of the offending material was then to forward it to all their friends back through the internal servers of the company and out

into cyber space. It may be better to adopt "*a better to be safe than sorry*" attitude in this regard.

Aside from pornography the Law also explicitly prohibits gambling, defamation and slander, as well as threats of violence or just threats generally.

Furthermore, the Law prohibits the spreading of lies that are likely to result in a loss to consumers partaking in an electronic transaction. The Law also prohibits the spreading of information that is likely to lead to clashes between groups based on matters of race, ethnicity, and religion, among others.

The Law also explicitly prohibits the sending of threats or other information that is intended to cause fear in the receiver of that information.

Hacking in all its forms are prohibited with the simple provision that prohibits access by any means by anyone to the electronic system of another. This is then elaborated to include specific motivations such as to obtain personal data and information. The Law also prohibits interception of electronic documents and the tapping of electronic communications. These provisions obviously include exceptions in order to facilitate the work of law enforcement.

Piracy in all its forms also is prohibited. This includes the standard prohibitions against the piracy of hardware and software but also includes the reproduction of computer codes access codes, among others.

Criminal Sanctions

The Law provides for terms of imprisonment up to 12 years and fines of up to IDR 12 billion for the standard breaches noted earlier. However, where there are aggravating circumstances these terms of imprisonment and fines can be extended by a 1/3 or 2/3 depending on the breach and who it is committed against.

Closing Provisions

The closing provisions provide that all of the subsidiary legislation that is required to give force to this Law must be issued and enacted no later than two years after the law comes in to force. This law will come into full force once signed by the President or after 30 days from 25 March 2008.

Conclusion

It is clear from the provisions in the new Law that the government is taking seriously the need to regulate in the sphere of cyber space. The reality is that as time passes more and more of peoples' personal and professional lives will be conducted online. The impact is that over time governments' are also going to have to provide more and more of their public services online to satisfy the demand of people not wanting to travel to a government office to complete a form or apply for a permit.

This in turn means that there will be vast amounts of personal information, whether it be about individuals or corporations that if abused would conceivably result in very significant losses.

Therefore, this is a responsible piece of legislation. It may not be perfect and some of the imperfections have been alluded to in this ILD, but in comparison to a completely unregulated area of law, this is a significant improvement.