CLIENT UPDATE
27 DECEMBER 2016

Electronic Information & Transactions Law Gets Makeover

Introduction

The House of Representatives ("**DPR**") recently enacted a number of important amendments to the Electronic Information and Transactions Law 2008 ("**EITL**"),[1] which has been a source of considerable controversy since it was first placed on the statute books. The amendments[2] address five principal issues:

1. Cyber defamation
2. Right to be Forgotten or Right of Erasure
3. Admissibility of electronic evidence
4. Government supervision
5. Investigation of Suspected Offences

Given the ubiquitous presence and importance of the Internet and social media in modern life, we propose to discuss these five issues in some detail in this Client Update.

1. Cyber Defamation

Throughout modern legal history, there has been tension between the freedom of expression, on one hand, and the right to have one's good name and reputation protected, on the other. This tension has been exacerbated by the emergence of the Internet and social media. Defamation remains a crime in many civil law jurisdictions (indeed, the majority of legal systems in East and Southeast Asia treat it as such). By contrast, common law jurisdictions generally regard defamation as a civil matter, with defamers being punished by the awarding of monetary damages.

In Indonesia, defamation continues to be a criminal offense (with a subsidiary claim for damages being available under the Civil Code). This is reflected in the controversial Article 27(3) of the EITL, which applies to "whosoever, deliberately and without lawful right, distributes and/or transmits and/or makes accessible electronic information and/or an electronic document that contains insulting and/or defamatory material." Under Article 45(1) EITL (prior to amendment), the offense carried a maximum term of imprisonment of six years and a fine of up to Rp 1 billion.

The controversy that has dogged Article 27(3) is focused not so much on the criminalization of defamation (there is little or no debate in Indonesia as to whether or not defamation should come within the realm of the criminal law), but rather the fact that, prior to the EITL's amendment, the maximum permissible term of imprisonment for a violation of Article 27(3) was six years. This allowed the Police to apply pre-trial detainment to suspected defamers as one of the requirements for detainment under the Civil Procedures Code is that the alleged offense carries a term of imprisonment of five years or more.

The principal problem in this regard is that the pre-trial detainment mechanism has become distorted in Indonesia. The virtual absence of a control mechanism has led to a situation where detainment is almost always resorted to. In fact, the situation has become so bad that the public automatically assumes that pressure has been brought to bear if a suspect is not detained.

[1] *Undang-undang No. 11/2008 tentang Informasi dan Transaksi Elektronik*
[2] Set out in *Undang-undang No. 19/2016 tentang Perubahan Atas UU No. 11/2008 tentang Informasi dan Transaksi Elekronik*

Presumably as a result of the public outcry over a series of controversies surrounding detainment under the EITL since 2008, the amended EITL reduces the maximum sentence for cyber defamation to four years, meaning that the Police will no longer be able to detain suspects for Article 27(3) offenses. Further, the amended Elucidation on Article 27(3) clarifies that the offense of cyber defamation is subject to the normal principles governing defamation under the Criminal Code (this had previously been confirmed by the Constitutional Court[3]). While these changes represent progress, everything in the garden is not yet rosy as the Police often charge suspects with multiple, related offenses. Thus, even though an individual may no longer be detained for an Article 27(3) offense, he or she could still be detained under other related articles, such as Article 36, which covers, inter alia, cyber defamation that causes actual loss to third parties – this carries a maximum prison term of 12 years and a fine of up to Rp 12 billion (Article 51(2) EITL).

It is interesting to note in this regard that the sanctions for defamation in the colonial-era Criminal Code (which entered into force in 1918 and continues to be the principal source of criminal law in Indonesia today), are much less draconian than those under the EITL. For example, the maximum punishment for slander (defamation using the spoken word) under Article 310(1) of the Criminal Code is nine months, while libel (defamation using the written word) carries a maximum prison term of one year and four months under Article 310(2). Although the reach of the Internet and its potential to spread defamatory content are virtually unlimited, it is nevertheless difficult to comprehend why there should be such dramatic differences in the sanctions for cyber defamation and those for "traditional" defamation."

2. "Right to Be Forgotten"

As with defamation, the "right to be forgotten" ("**RTBF**") or "right of erasure" issue gives rise to fundamental questions concerning the public's right to information versus the individual's right to privacy. The concept, which has been pioneered in the European Union, became the subject of international discourse following a ruling of the European Court of Justice on 13 May 2014, in which the Court legally formalized the "right to be forgotten" as a human right.[4]

In 2016, the European Union adopted its General Data Protection Regulation, which comes into force in 2018. The Regulation enshrines the right to be forgotten / right of erasure in Article 17, subject to a number of exemptions that, inter alia, include (i) exercising the right of freedom of expression and information; (ii) for reasons of public interest in the area of public health; (iii) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes [...]; and (iv) for the establishment, exercise or defence of legal claims.

Article 26 of the amended EITL contains three new subsections (subsections 3, 4 and 5), which establish the right to be forgotten in Indonesian law for the first time.

The new right requires an electronic system provider to erase electronic information or a document that is (i) no longer relevant, (ii) under its control, (iii) pursuant to request of a data owner, and (iv) based on a court order. It is further stated that the right will be provided for in greater detail by Government Regulation.

At least two points will need to be further clarified in this regard. First, how will relevancy be defined? Will parameters be provided or will this be left entirely up to the court? The second issue that will require clarification is whether the request and court order requirements are cumulative, i.e., whether a request for removal can only be made after a court order is sought?

In a related development, the right to request the removal of personal data is provided for in a recently issued Minister of Communication and Information Regulation on personal data protection. An AHP Client Update on the regulation will be provided separately.

---

[3] Decision No. 50/PUU-VI/2008

[4] *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González* (2014).

3. Admissibility of Electronic Evidence

The issue of the admissibility of electronic evidence came to the fore in the run-up to the amendment of the EITL following a Constitutional Court decision[5] on a petition brought by the former (and recently reappointed) speaker of the DPR. The background to the petition may be briefly summarized as follows: The petitioner attended a meeting with representatives of a major mining company. What was said at the meeting was secretly recorded by one of the key participants - a senior officer of the mining company. The recording appeared to show the petitioner inviting the mining company to participate in a corrupt conspiracy. The Prosecution Service then used the recording to launch an investigation.

The petitioner argued that the recording should not be admitted in evidence as he claimed it had been illegally obtained in breach of Article 31 EITL, which prohibits the interception or bugging (hacking) of electronic information or an electronic document stored on a computer or in an electronic system, save in the case of an interception conducted in the law enforcement context at the request of the Police, Prosecution Service or other law enforcement authority designated by law. As pointed out by the Government in its submission, it is difficult in the extreme to envisage how the making of a tape recording of a conversation during a meeting could come within the scope of this offense.

Despite the obvious inconsistency in the petitioner's argument, the majority of the Constitutional Court accepted it, holding that electronic information or an electronic document (including a tape recording) could only be admitted as evidence in the law enforcement context if it were obtained at the request of the Police, Prosecution Service or other law enforcement authority designated by law. This meant that a secretly recorded conversation would no longer be admissible in a criminal prosecution.

This Constitutional Court's decision in this case may best be described as regrettable. Not surprisingly, it was roundly criticized by independent observers for its inconsistency, strained logic and apparently contrived nature, not to mention a pronounced lack of clarity as to its scope. Did it, for example, preclude the admission in evidence of a CCTV recording of a murder or rape? The answer would appear to be yes. Despite this apparent absurdity, the judgment was final and conclusive. There could be no appeal.

The decision has now been effectively circumvented through the amendment of the Elucidation on Article 5(2) EITL. This is because a Constitutional Court judgment only applies to the provision that is impugned before the Court. Given that Article 5(2) has now been amended through its Elucidation, the decision now longer applies to it. The amended text reads as follows:

"In the particular case of Electronic Information and/or an Electronic Document that results from interception or bugging, or a recording that forms part of a bugging [exercise], it must be obtained in the context of law enforcement at the request of the Police, Prosecution Service and/or other institution designated by law."
If we go by the normal rules of language and grammar, the amended text does not cover secretly made tape recordings of private conversations. Accordingly, it would seem that such recordings are once again admissible as evidence in criminal proceedings.

By way of comparison, under U.S. Federal law, a recorded conversation may be admitted as evidence provided that one party to the conversation, which may be the party making the recording (so long as that person participated in the conversation), consented to the recording.

In other jurisdictions, a secretly obtained private recording will often be admitted if the desirability of admitting the recording outweighs the undesirability of admitting material obtained in that particular way. Another test applied turns on the nature of the offence charged. The more serious the offence, the stronger the argument for admissibility.

Overall, it may be stated that it is very rare indeed internationally for secretly obtained recordings of private conversations to be completely excluded from admissibility as evidence in criminal cases.

[5] Decision No. 20/PUU-XIV/2016

4. Government supervision

Few would argue that unrestricted internet freedom is suitable for Indonesia. In common with many post-colonial states, the country is characterized by a complex religious, ethnic and racial mix, where the slightest perceived insult can trigger often violent unrest. Accordingly, most would agree that the Government is fully justified in attempting to keep the lid on what is posted on the internet or disseminated via social media. However, there continues to be a debate as to how this may best be achieved. The Government argues that it should have the final say as to what should or should not be permitted, while freedom of expression advocates and the media argue that judicial supervision is necessary.

The amended Article 40 EITL reflects the Government's stance on the issue by extending its powers "to protect the public interest, in accordance with law, against all disruptions to public order arising out of the abuse of electronic information or transactions." These extended powers authorize the Government to "prevent the dissemination and use of electronic information or electronic documents that contain prohibited content, as determined by law" and "in the conducting of such preventive action, to terminate access to, or order an electronic system provider to terminate access to, electronic information or electronic documents that contain prohibited content."

The Government's supervisory powers are further reinforced by Article 43(5) h, which authorizes designated civil service investigators to block access to "electronic systems or data" that are implicated in criminal offenses.

It should be noted that the Government's Internet supervisory powers are nothing new. Lower level regulations accord similar powers to the Government. For example, Minister of Communications and Information Technology Regulation No. 19 of 2014 (on the Control of Internet Websites Containing Negative Content), which authorizes the Government to maintain a list of websites that contain pornography or other illegal content and to require internet service providers to block them.

However, these powers have now been further extended and been placed on a statutory footing.
Besides giving the Government a stronger legal basis for blocking access to prohibited content, the amended EITL also gives it the power to reach electronic information beyond websites. Given that the definition of "prohibited content" might be debatable and the extent of the Government reach might be challengeable, the amended EITL states that these issues will be further provided for by Government Regulation.

5. Investigation of Suspected Offenses

The amended EITL contains a number of changes that are designed to bring investigative procedures in the cyber sphere into line with the Criminal Procedures Code, including a new requirement that the "searching or seizing" of an electronic system must be conducted in accordance with the provisions of the Criminal Procedures Code, rather than based upon a court order.

Similarly, arrests and detainments must now also be conducted based on the provisions of the Criminal Procedures Code, whereas previously an investigator in conducting an arrest or detainment needed to secure a court order within 24 hours. By contrast, the Criminal Procedures Code does not require a court order for the conducting of an arrest and/or detainment. This aspect is discussed in greater detail in Section 1 above.

Contacts

Eko Ahmad Ismail Basyuni
Partner
Mergers & Acquisitions

D (62) 21 2555 7802
F (62) 21 2555 7899
eko.basyuni@ahp.co.id

Zacky Zainal Husein
Partner
Mergers & Acquisitions

D (62) 21 2555 9956
F (62) 21 2555 7899
zacky.husein@ahp.co.id

ASEAN Economic Community Portal

With the launch of the ASEAN Economic Community ("**AEC**") in December 2015, businesses looking to tap the opportunities presented by the integrated markets of the AEC can now get help a click away. Rajah & Tann Asia, United Overseas Bank and RSM Chio Lim Stone Forest, have teamed up to launch "Business in ASEAN", a portal that provides companies with a single platform that helps businesses navigate the complexities of setting up operations in ASEAN.

By tapping into the professional knowledge and resources of the three organisations through this portal, small- and medium-sized enterprises across the 10-member economic grouping can equip themselves with the tools and know-how to navigate ASEAN's business landscape. Of particular interest to businesses is the "Ask a Question" feature of the portal which enables companies to pose questions to the three organisations which have an extensive network in the region. The portal can be accessed at http://www.businessinasean.com/.

Our regional presence

Our regional contacts

RAJAH & TANN | *Singapore*

Rajah & Tann Singapore LLP
9 Battery Road #25-01
Straits Trading Building
Singapore 049910
T +65 6535 3600 F +65 6225 9630
sg.rajahtannasia.com

R&T SOK & HENG | *Cambodia*

R&T Sok & Heng Law Office
Vattanac Capital Office Tower, Level 17, No. 66
Preah Monivong Boulevard, Sangkat Wat Phnom
Khan Daun Penh, 12202 Phnom Penh, Cambodia
T +855 23 963 112 / 113 F +855 963 116
kh.rajahtannasia.com
**in association with Rajah & Tann Singapore LLP*

RAJAH & TANN REPRESENTATIVE OFFICE | *China*

Rajah & Tann Singapore LLP
Shanghai Representative Office
Unit 1905-1906, Shui On Plaza, 333 Huai Hai Middle Road
Shanghai 200021, People's Republic of China
T +86 21 6120 8818 F +86 21 6120 8820
cn.rajahtannasia.com

RAJAH & TANN NK LEGAL | *Myanmar*

Rajah & Tann NK Legal Myanmar Company Limited
Myanmar Centre Tower 1, Floor 07, Unit 08,
192 Kaba Aye Pagoda Road, Bahan Township,
Yangon, Myanmar
T +95 9 73040763 / +95 1 657902 / +95 1 657903
F +95 1 9665537
mm.rajahtannasia.com

ASSEGAF HAMZAH & PARTNERS | *Indonesia*

ASSEGAF HAMZAH & PARTNERS | *Indonesia*

Assegaf Hamzah & Partners

Jakarta Office
Menara Rajawali 16th Floor
Jalan DR. Ide Anak Agung Gde Agung Lot #5.1
Kawasan Mega Kuningan, Jakarta 12950, Indonesia
T +62 21 2555 7800 F +62 21 2555 7899
www.ahp.co.id

Surabaya Office
Pakuwon Center, Superblok Tunjungan City
Lantai 11, Unit 08
Jalan Embong Malang No. 1, 3, 5, Surabaya 60261, Indonesia
T +62 31 5116 4550 F +62 31 5116 4560

** Assegaf Hamzah & Partners is an independent law firm in Indonesia and a member of the Rajah & Tann Asia network.*

CHRISTOPHER & LEE ONG | *Malaysia*

Christopher & Lee Ong
Level 22, Axiata Tower, No. 9 Jalan Stesen Sentral 5,
Kuala Lumpur Sentral, 50470 Kuala Lumpur, Malaysia
T +60 3 2273 1919 F +60 3 2273 8310
www.christopherleeong.com
**in association with Rajah & Tann Singapore LLP*

RAJAH & TANN | *Thailand*

Rajah & Tann (Thailand) Limited
973 President Tower, 12th Floor, Units 12A-12F
Ploenchit Road, Lumpini, Pathumwan
Bangkok 10330, Thailand
T +66 2 656 1991 F +66 2 656 0833
th.rajahtannasia.com

RAJAH & TANN | *Lao PDR*

Rajah & Tann (Laos) Sole Co., Ltd.
Phonexay Village, 23 Singha Road, House Number 046/2
Unit 4, Saysettha District, Vientiane Capital, Lao PDR
T +856 21 454 239 F +856 21 285 261
la.rajahtannasia.com

RAJAH & TANN LCT LAWYERS | *Vietnam*

Rajah & Tann LCT Lawyers

Ho Chi Minh City Office
Saigon Centre, Level 13, Unit 2&3
65 Le Loi Boulevard, District 1, HCMC, Vietnam
T +84 8 3821 2382 / +84 8 3821 2673 F +84 8 3520 8206

Hanoi Office
Lotte Center Hanoi - East Tower, Level 30, Unit 3003,
54 Lieu Giai St., Ba Dinh Dist., Hanoi, Vietnam
T +84 4 3267 6127 F +84 4 3267 6128
www.rajahtannlct.com

Based in Jakarta, and consistently gaining recognition from independent observers, Assegaf Hamzah & Partners has established itself as a major force locally and regionally, and is ranked as a top-tier firm in many practice areas. Founded in 2001, it has a reputation for providing advice of the highest quality to a wide variety of blue-chip corporate clients, high net worth individuals, and government institutions.

Assegaf Hamzah & Partners is part of Rajah & Tann Asia, a network of local law firms in Singapore, Cambodia, China, Indonesia, Lao PDR, Malaysia, Myanmar, Thailand and Vietnam. Our Asian network also includes Singapore-based regional desks focused on Japan and South Asia.