Update: December 2016

UNDANG-UNDANG REPUBLIK INDONESIA
NOMOR 11 TAHUN 2008
TENTANG
INFORMASI DAN TRANSAKSI ELEKTRONIK

LAW OF THE REPUBLIC OF INDONESIA
NUMBER 11 OF 2008
CONCERNING
ELECTRONIC INFORMATION AND TRANSACTIONS

Diubah oleh UU No. 19 Tahun 2016
25 November 2016
(Dicetak tebal)

As amended by Law No. 19 of 2016
November 25, 2016
(Printed in bold face)

Daftar Isi / Table of Contents

NOTE: WHERE NO ELUCIDATION IS PROVIDED UNDERNEATH A CLAUSE, THE CLAUSE IS SUFFICIENTLY CLEAR.

Translated by Wishnu Basuki
wbasuki@gmail.com

UNDANG-UNDANG REPUBLIK INDONESIA
NOMOR 11 TAHUN 2008
TENTANG
INFORMASI DAN TRANSAKSI ELEKTRONIK

Sebagaimana diubah oleh UU No. 19 Tahun 2016 25 November 2016
(Dicetak tebal)

LAW OF THE REPUBLIC OF INDONESIA
NUMBER 11 OF 2008
CONCERNING
ELECTRONIC INFORMATION AND TRANSACTIONS

As amended by Law No. 19 of 2016 November 25, 2016
(Printed in bold face)

DENGAN RAHMAT TUHAN YANG MAHA ESA

PRESIDEN REPUBLIK INDONESIA,

Menimbang:

a. bahwa pembangunan nasional adalah suatu proses yang berkelanjutan yang harus senantiasa tanggap terhadap berbagai dinamika yang terjadi di masyarakat;

b. bahwa globalisasi informasi telah menempatkan Indonesia sebagai bagian dari masyarakat informasi dunia sehingga mengharuskan dibentuknya pengaturan mengenai pengelolaan informasi dan Transaksi Elektronik di tingkat nasional sehingga pembangunan Teknologi Informasi dapat dilakukan secara optimal, merata, dan menyebar ke seluruh lapisan masyarakat guna mencerdaskan kehidupan bangsa;

c. bahwa perkembangan dan kemajuan Teknologi Informasi yang demikian pesat telah menyebabkan perubahan kegiatan kehidupan manusia dalam berbagai bidang yang secara langsung telah memengaruhi lahirnya bentuk-bentuk perbuatan hukum baru;

d. bahwa penggunaan dan pemanfaatan Teknologi Informasi harus terus dikembangkan untuk menjaga, memelihara, dan memperkukuh persatuan dan kesatuan nasional berdasarkan peraturan perundang-undangan demi kepentingan nasional;

e. bahwa pemanfaatan Teknologi Informasi

WITH THE BLESSING OF GOD ALMIGHTY

THE PRESIDENT OF THE REPUBLIC OF INDONESIA,

Considering:

a. that the national development is a sustainable process that must at all times be responsive to the varying dynamics among the public;

b. that globalization of information has placed Indonesia as part of the world's information community, and this requires the making of regulation concerning organization of Electronic Information and transactions at the national level to enable the development of Information Technology to be carried out in an optimal, distributive, and widespread manner throughout all levels of the society to advance the intellectual life of the people;

c. that the very rapid development and advance of Information Technology have contributed to the changes in the people's life activities in the various fields that have had a direct effect on the emergence of new forms of legal acts;

d. that the use and utilization of Information Technology must continuously be developed to foster, maintain, and strengthen the national union and unity under the laws and regulations in the national interest;

e. that utilization of Information Technology

berperan penting dalam perdagangan dan pertumbuhan perekonomian nasional untuk mewujudkan kesejahteraan masyarakat;

f. bahwa Pemerintah perlu mendukung pengembangan Teknologi Informasi melalui infrastruktur hukum dan pengaturannya sehingga pemanfaatan Teknologi Informasi dilakukan secara aman untuk mencegah penyalahgunaannya dengan memperhatikan nilai-nilai agama dan sosial budaya masyarakat Indonesia;

g. bahwa berdasarkan pertimbangan-pertimbangan sebagaimana dimaksud dalam huruf a, huruf b, huruf c, huruf d, huruf e, dan huruf f perlu membentuk Undang-undang tentang Informasi dan Transaksi Elektronik.

Mengingat:

Pasal 5 ayat (1) dan Pasal 20 Undang-Undang Dasar Negara Republik Indonesia Tahun 1945;

Dengan Persetujuan Bersama
DEWAN PERWAKILAN RAKYAT
REPUBLIK INDONESIA
dan
PRESIDEN REPUBLIK INDONESIA

MEMUTUSKAN:

Menetapkan: UNDANG-UNDANG TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK.

PENJELASAN UMUM

Pemanfaatan Teknologi Informasi, media, dan komunikasi telah mengubah baik perilaku masyarakat maupun peradaban manusia secara global. Perkembangan teknologi informasi dan komunikasi telah pula menyebabkan hubungan dunia menjadi tanpa batas (borderless) dan menyebabkan perubahan sosial, ekonomi, dan budaya secara signifikan berlangsung demikian cepat. Teknologi Informasi saat ini menjadi pedang bermata dua karena selain memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan, dan peradaban manusia, sekaligus menjadi sarana efektif perbuatan melawan hukum.

Saat ini telah lahir suatu rezim hukum baru yang dikenal dengan hukum siber atau hukum

assumes the important role in national trade and economic growth in order to achieve public prosperity;

f. that the Government needs to support the development of Information Technology through infrastructure of law and its regulation to enable the Information Technology being utilized securely to prevent its misuse with due regard to the religious and social-cultural values of the Indonesian society;

g. that in consideration of point (a), point (b), point (c), point (d), point (e), and point (f), it is necessary to make Law concerning Electronic Information and Transactions.

Bearing in Mind:

Article 5 section (1) and Article 20 of the 1945 Constitution of the Republic of Indonesia;

With the Joint Consent of
THE HOUSE OF REPRESENTATIVES OF
THE REPUBLIC OF INDONESIA
and
THE PRESIDENT OF THE REPUBLIC OF INDONESIA

HAS DECIDED:

To enact: LAW CONCERNING ELECTRONIC INFORMATION AND TRANSACTIONS.

GENERAL ELUCIDATION

Utilization of Information Technology, media, and communications has globally changed both public behavior and human civilization. The development of information technology and communications has also contributed to make the world connection borderless and has significantly made social, economic, and cultural changes rapidly. Today, Information Technology serves as a double-edged sword, that is, to give contributions to the improvement of human welfare, advance, and civilization, and simultaneously becomes effective means for unlawful acts.

Today, a regime of a new law is born, known as hukum siber *or telematics law.* Hukum siber *or*

telematika. Hukum siber atau cyber law secara internasional digunakan untuk istilah hukum yang terkait dengan pemanfaatan teknologi informasi dan komunikasi. Demikian pula, hukum telematika yang merupakan perwujudan dari konvergensi hukum telekomunikasi, hukum media, dan hukum informatika. Istilah lain yang juga digunakan adalah hukum teknologi informasi (law of information technology), hukum dunia maya (virtual world law) dan hukum mayantara. Istilah-istilah tersebut lahir mengingat kegiatan yang dilakukan melalui jaringan sistem komputer dan sistem komunikasi baik dalam lingkup lokal maupun global (Internet) dengan memanfaatkan teknologi informasi berbasis sistem komputer yang merupakan sistem elektronik yang dapat dilihat secara virtual. Permasalahan hukum yang seringkali dihadapi adalah ketika terkait dengan penyampaian informasi, komunikasi, dan/atau transaksi secara elektronik, khususnya dalam hal pembuktian dan hal yang terkait dengan perbuatan hukum yang dilaksanakan melalui sistem elektronik.

cyber law is internationally used as a legal term concerning the utilization of information technology and communications. Likewise, telematics law is the embodiment of the convergence of telecommunications law, media law, and informatics law. Other terms also used are hukum teknologi informasi *(law of information technology),* hukum dunia maya *(virtual world law) and* hukum mayantara. *Such terms were coined after activities carried out through computer system networks and communications systems in the scope of both local and global (Internet) by taking advantage of computer system-based information technology that constitutes virtually-visible electronic systems. Legal issues frequently faced are when those involve the conveyance of information, communications, and/or transactions in an electronic manner, especially a matter of proof and matters that concern legal acts committed by means of electronic systems.*

Yang dimaksud dengan sistem elektronik adalah sistem komputer dalam arti luas, yang tidak hanya mencakup perangkat keras dan perangkat lunak komputer, tetapi juga mencakup jaringan telekomunikasi dan/atau sistem komunikasi elektronik. Perangkat lunak atau program komputer adalah sekumpulan instruksi yang diwujudkan dalam bentuk bahasa, kode, skema, ataupun bentuk lain, yang apabila digabungkan dengan media yang dapat dibaca dengan komputer akan mampu membuat komputer bekerja untuk melakukan fungsi khusus atau untuk mencapai hasil yang khusus, termasuk persiapan dalam merancang instruksi tersebut.

Electronic systems mean computer systems in a broad sense that include not only computer hardware and software, but also telecommunications networks and/or electronic communications systems. Software or a computer program is a collection of instructions embodied in the form of language, code, scheme, or other forms when interfaced with computer-readable media is able to make computers work to execute special functions or to deliver special results, including preparation in writing such instructions.

Sistem elektronik juga digunakan untuk menjelaskan keberadaan sistem informasi yang merupakan penerapan teknologi informasi yang berbasis jaringan telekomunikasi dan media elektronik, yang berfungsi merancang, memproses, menganalisis, menampilkan, dan mengirimkan atau menyebarkan informasi elektronik. Sistem informasi secara teknis dan manajemen sebenarnya adalah perwujudan penerapan produk teknologi informasi ke dalam suatu bentuk organisasi dan manajemen sesuai dengan karakteristik kebutuhan pada organisasi tersebut dan sesuai dengan tujuan peruntukannya. Pada sisi yang lain, sistem informasi secara teknis dan fungsional adalah keterpaduan sistem antara manusia dan mesin yang mencakup komponen perangkat keras, perangkat lunak, prosedur, sumber daya manusia, dan substansi informasi

Electronic systems are also used to explain the existence of information systems that constitute application of telecommunications network-based information technology and electronic media, serving to write, process, analyze, display, and send or distribute electronic information. Technically or in management respect, information systems are in effect the embodiment of application of information technology products in some form of organization and management fitting the typical needs within such organization and conforming to the purpose of the functions. On the other hand, technically and functionally speaking, information systems are systems that integrate human into machines including hardware components, software, procedures, human resources, and substance of information that in their utilization include functions of input,

yang dalam pemanfaatannya mencakup fungsi input, process, output, storage, dan communication.

process, output, storage, and communications.

Sehubungan dengan itu, dunia hukum sebenarnya sudah sejak lama memperluas penafsiran asas dan normanya ketika menghadapi persoalan kebendaan yang tidak berwujud, misalnya dalam kasus pencurian listrik sebagai perbuatan pidana. Dalam kenyataan kegiatan siber tidak lagi sederhana karena kegiatannya tidak lagi dibatasi oleh teritori suatu negara, yang mudah diakses kapanpun dan dari manapun. Kerugian dapat terjadi baik pada pelaku transaksi maupun pada orang lain yang tidak pernah melakukan transaksi, misalnya pencurian dana kartu kredit melalui pembelanjaan di Internet. Di samping itu, pembuktian merupakan faktor yang sangat penting, mengingat informasi elektronik bukan saja belum terakomodasi dalam sistem hukum acara Indonesia secara komprehensif, melainkan juga ternyata sangat rentan untuk diubah, disadap, dipalsukan dan dikirim ke berbagai penjuru dunia dalam waktu hitungan detik. Dengan demikian, dampak yang diakibatkannyapun bisa demikian kompleks dan rumit.

As aforesaid, it is true the world of law has long since broadened its interpretation of principles and values when facing intangible issues, for example, the criminalization of electricity theft. Facts of cyber activities are no longer that simple in that such activities can no longer be bordered by a state's territory, the access to which is easily made at any time and from anywhere. Loss may be sustained by both transacting actors and other persons who never enter transactions, for example, credit card frauds by internet shopping. In addition, proof is a crucial factor since not only has electronic information been unaccommodated comprehensively by the Indonesian law of civil procedure, but in fact, also vulnerable to alteration, interception, forge and transmission to various places worldwide in second. So, the impacts as consequence may be very complex and complicated.

Permasalahan yang lebih luas terjadi pada bidang keperdataan karena transaksi elektronik untuk kegiatan perdagangan melalui sistem elektronik (electronic commerce) telah menjadi bagian dari perniagaan nasional dan internasional. Kenyataan ini menunjukkan bahwa konvergensi di bidang teknologi informasi, media, dan informatika (telematika) berkembang terus tanpa dapat dibendung, seiring dengan ditemukannya perkembangan baru di bidang teknologi informasi, media, dan komunikasi.

Broader issues also appear in the private sphere in which electronic transactions for trade by means of electronic systems (electronic commerce) have made a part of national and international trade. This fact shows that the convergence in the field of information technology, media, and informatics (telematics), inevitably, keeps developing in line with the invention in the field of information technology, media, and communications.

Kegiatan melalui media sistem elektronik, yang disebut juga ruang siber (cyber space), meskipun bersifat virtual dapat dikategorikan sebagai tindakan atau perbuatan hukum yang nyata. Secara yuridis kegiatan pada ruang siber tidak dapat didekati dengan ukuran dan kualifikasi hukum konvensional saja sebab jika cara ini yang ditempuh akan terlalu banyak kesulitan dan hal yang lolos dari pemberlakuan hukum. Kegiatan dalam ruang siber adalah kegiatan virtual yang berdampak sangat nyata meskipun alat buktinya bersifat elektronik.

Activities via electronic media systems also called cyber (cyberspace), despite being virtual, can be categorized as actual legal acts and actions. Judicially speaking, activities in cyberspace cannot be approached by parameters and qualifications of conventional law only, and if adopted such conventional method, it is too complicated and many would evade the law. Activities in cyberspace are virtual activities that have actual impacts despite the means of proof being electronic in nature.

Dengan demikian, subjek pelakunya harus dikualifikasikan pula sebagai Orang yang telah melakukan perbuatan hukum secara nyata. Dalam kegiatan e-commerce antara lain dikenal adanya dokumen elektronik yang kedudukannya

As aforesaid, the subject actor must be qualified as a Person who has committed an actual legal act. In e-commerce activities, there are such things known as, inter alia, electronic records, the position of which is held equivalent to documents

disetarakan dengan dokumen yang dibuat di atas kertas.

Berkaitan dengan hal itu, perlu diperhatikan sisi keamanan dan kepastian hukum dalam pemanfaatan teknologi informasi, media, dan komunikasi agar dapat berkembang secara optimal. Oleh karena itu, terdapat tiga pendekatan untuk menjaga keamanan di cyber space, yaitu pendekatan aspek hukum, aspek teknologi, aspek sosial, budaya, dan etika. Untuk mengatasi gangguan keamanan dalam penyelenggaraan sistem secara elektronik, pendekatan hukum bersifat mutlak karena tanpa kepastian hukum, persoalan pemanfaatan teknologi informasi menjadi tidak optimal.

BAB I

KETENTUAN UMUM

Pasal 1

Dalam Undang-Undang ini yang dimaksud dengan:

1. "Informasi Elektronik" adalah satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, *electronic data interchange* (EDI) surat elektronik (*electronic mail*), telegram, teleks, *telecopy* atau sejenisnya, huruf, tanda, angka, Kode Akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya.

2. "Transaksi Elektronik" adalah perbuatan hukum yang dilakukan dengan menggunakan Komputer, jaringan Komputer, dan/atau media elektronik lainnya.

3. "Teknologi Informasi" adalah suatu teknik untuk mengumpulkan, menyiapkan, menyimpan, memproses, mengumumkan, menganalisis, dan/atau menyebarkan informasi.

4. "Dokumen Elektronik" adalah setiap Informasi Elektronik yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal, atau sejenisnya, yang dapat dilihat, ditampilkan dan/atau didengar melalui Komputer atau Sistem Elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto atau sejenisnya,

made on paper.

In connection therewith, attention to security and legal certainty in the utilization of information technology, media, and communications is necessary to be paid to enable optimal development. There are accordingly three approaches to maintain cyberspace security, i.e., approaches of legal aspect, technological aspect, and social, cultural, and ethics aspect. To address security threats in the provision of electronic systems, a legal approach is absolute because without legal certainty the problems of the utilization of information technology cannot be addressed in an optimum manner.

CHAPTER I

GENERAL PROVISIONS

Article 1

In this Law:

1. "Electronic Information" means one cluster or clusters of electronic data, including but not limited to writings, sounds, images, maps, drafts, photographs, electronic data interchange (EDI), electronic mails, telegrams, telex, telecopy or the like, letters, signs, figures, Access Codes, symbols or perforations that have been processed for meaning or are intelligible to persons who are able to understand them.

2. "Electronic Transaction" means a legal act that is committed by using Computers, Computer networks, and/or other electronic media.

3. "Information Technology" means a technique to collect, prepare, store, process, announce, analyze, and/or disseminate information.

4. "Electronic Record" means any Electronic Information that is created, forwarded, sent, received, or stored in analog, digital, electromagnetic, optical form, or the like, visible, displayable and/or audible via Computers or Electronic Systems, including but not limited to writings, sounds, images, maps, drafts, photographs or the like, letters, signs, figures, Access Codes, symbols or

huruf, tanda, angka, Kode Akses, simbol atau perforasi yang memiliki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya.	perforations having certain meaning or definition or intelligible to persons who are able to understand them.
5. "Sistem Elektronik" adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan Informasi Elektronik.	5. "Electronic System" means a set of electronic devices and procedures that serve to prepare, collect, process, analyze, store, display, announce, send, and/or disseminate Electronic Information.
6. "Penyelenggaraan Sistem Elektronik" adalah pemanfaatan Sistem Elektronik oleh penyelenggara negara, Orang, Badan Usaha, dan/atau masyarakat.	6. "Provision of Electronic System" means utilization of Electronic System by the state administrators, Persons, Business Entities, and/or the public.
6a. "Penyelenggara Sistem Elektronik" adalah setiap Orang, penyelenggara negara, Badan Usaha, dan masyarakat yang menyediakan, mengelola, dan/atau mengoperasikan Sistem Elektronik, baik secara sendiri-sendiri maupun bersama-sama kepada pengguna Sistem Elektronik untuk keperluan dirinya dan/atau keperluan pihak lain.	**6a. "Electronic System Provider" means any Person, state administrator, Business Entity, and the public who provide, administer, and/or operate an Electronic System, whether individually or jointly, for Electronic System users for their own use and/or for use by other parties.**
7. "Jaringan Sistem Elektronik" adalah terhubungnya dua Sistem Elektronik atau lebih, yang bersifat tertutup ataupun terbuka.	7. "Electronic System Network" means a closed or open connection of two or more Electronic Systems.
8. "Agen Elektronik" adalah perangkat dari suatu Sistem Elektronik yang dibuat untuk melakukan suatu tindakan terhadap suatu Informasi Elektronik tertentu secara otomatis yang diselenggarakan oleh Orang.	8. "Electronic Agent" means an automated electronic means that is used to initiate an action to certain Electronic Information, which is operated by a Person.
9. "Sertifikat Elektronik" adalah sertifikat yang bersifat elektronik yang memuat Tanda Tangan Elektronik dan identitas yang menunjukan status subyek hukum para pihak dalam Transaksi Elektronik yang dikeluarkan oleh Penyelenggara Sertifikasi Elektronik.	9. "Electronic Certificate" means a certificate in electronic nature that bears an Electronic Signature and identity demonstrating a status of a legal subject of parties to an Electronic Transaction issued by Certification Service Providers.
10. "Penyelenggara Sertifikasi Elektronik" adalah badan hukum yang berfungsi sebagai pihak yang layak dipercaya, yang memberikan dan mengaudit Sertifikat Elektronik.	10. "Electronic Certification Service Provider" means a legal entity that acts as a reliable party, issues and audits Electronic Certificates.
11. "Lembaga Sertifikasi Keandalan" adalah lembaga independen yang dibentuk oleh profesional yang diakui, disahkan, dan diawasi oleh Pemerintah dengan kewenangan mengaudit dan mengeluarkan sertifikat	11. "Trustworthiness Certification Institution" means an independent institution that is formed by professionals acknowledged, certified, and supervised by the Government, whose competence is to audit and issue

keandalan dalam Transaksi Elektronik.

trustworthiness certificates for Electronic Transactions.

12. "Tanda Tangan Elektronik" adalah tanda tangan yang terdiri atas Informasi Elektronik yang dilekatkan, terasosiasi atau terkait dengan Informasi Elektronik lainnya yang digunakan sebagai alat verifikasi dan autentikasi.

12. "Electronic Signature" means a signature that contains Electronic Information that is attached to, associated or linked with other Electronic Information that is used for means of verification and authentication.

13. "Penanda Tangan" adalah subyek hukum yang terasosiasikan atau terkait dengan Tanda Tangan Elektronik.

13. "Signatory/Signer" means a legal subject associated or linked with an Electronic Signature.

14. "Komputer" adalah alat untuk memproses data elektronik, magnetik, optikal, atau sistem yang melaksanakan fungsi logika, aritmatika, dan penyimpanan.

14. "Computer" means an electronic, magnetic, optical data processing device, or a system that performs logic, arithmetic, and storage functions.

15. "Akses" adalah kegiatan melakukan interaksi dengan Sistem Elektronik yang berdiri sendiri atau dalam jaringan.

15. "Access" means an activity to make interaction with independent or network Electronic Systems.

16. "Kode Akses" adalah angka, huruf, simbol, karakter lainnya atau kombinasi di antaranya yang merupakan kunci untuk dapat mengakses Komputer dan/atau Sistem Elektronik lainnya.

16. "Access Code" means a figure, letter, symbol, other character or a combination thereof, which is a key to enable Access to Computers and/or other Electronic Systems.

17. "Kontrak Elektronik" adalah perjanjian para pihak yang dibuat melalui Sistem Elektronik.

17. "Electronic Contract" means an agreement of parties entered into by means of Electronic Systems.

18. "Pengirim" adalah subyek hukum yang mengirimkan Informasi Elektronik dan/atau Dokumen Elektronik.

18. "Sender/Originator" means a legal subject that sends Electronic Information and/or Electronic Records.

19. "Penerima" adalah subyek hukum yang menerima Informasi Elektronik dan/atau Dokumen Elektronik dari Pengirim.

19. "Recipient/Addressee" means a legal subject that receives Electronic Information and/or Electronic Records from Senders/Originators.

20. "Nama Domain" adalah alamat internet penyelenggara negara, Orang, Badan Usaha, dan/atau masyarakat, yang dapat digunakan dalam berkomunikasi melalui internet, yang berupa kode atau susunan karakter yang bersifat unik untuk menunjukkan lokasi tertentu dalam internet.

20. "Domain Name" means an internet address of a state administrator, Person, Business Entity, and/or the public that can be used for communication over the internet, in the form of unique character code or set to identify a certain location on the internet.

21. "Orang" adalah orang perseorangan, baik warga negara Indonesia, warga negara asing maupun badan hukum.

21. "Person" means an individual, whether an Indonesian citizen, foreign citizen, or legal entity.

22. "Badan Usaha" adalah perusahaan perseorangan atau perusahaan persekutuan,

22. "Business Entity" means a sole proprietorship or partnership of both legal entity and non-

baik yang berbadan hukum maupun yang tidak berbadan hukum.

23. "Pemerintah" adalah Menteri atau pejabat lainnya yang ditunjuk oleh Presiden.

Pasal 2

Undang-Undang ini berlaku untuk setiap Orang yang melakukan perbuatan hukum sebagaimana diatur dalam Undang-Undang ini, baik yang berada di wilayah hukum Indonesia maupun di luar wilayah hukum Indonesia, yang memiliki akibat hukum di wilayah hukum Indonesia dan/atau di luar wilayah hukum Indonesia dan merugikan kepentingan Indonesia.

Penjelasan Pasal 2:

Undang-Undang ini memiliki jangkauan yurisdiksi tidak semata-mata untuk perbuatan hukum yang berlaku di Indonesia dan/atau dilakukan oleh warga negara Indonesia, tetapi juga berlaku untuk perbuatan hukum yang dilakukan di luar wilayah hukum (yurisdiksi) Indonesia baik oleh warga negara Indonesia maupun oleh warga negara asing atau badan hukum Indonesia maupun badan hukum asing yang memiliki akibat hukum di Indonesia, mengingat pemanfaatan Teknologi Informasi untuk Informasi Elektronik dan Transaksi Elektronik dapat bersifat lintas teritorial atau universal.

Yang dimaksud dengan "merugikan kepentingan Indonesia" adalah meliputi tetapi tidak terbatas pada merugikan kepentingan ekonomi nasional, perlindungan data strategis, harkat dan martabat bangsa, pertahanan dan keamanan negara, kedaulatan negara, warga negara, serta badan hukum Indonesia.

BAB II

ASAS DAN TUJUAN

Pasal 3

Pemanfaatan Teknologi Informasi dan Transaksi Elektronik dilaksanakan berdasarkan asas kepastian hukum, manfaat, kehati-hatian, iktikad baik, dan kebebasan memilih teknologi atau netral teknologi.

Penjelasan Pasal 3:

"Asas kepastian hukum" berarti landasan hukum bagi pemanfaatan Teknologi Informasi dan Transaksi Elektronik serta segala sesuatu yang

legal entity.

23. "Government" means a Minister(s) or other official(s) the President designates.

Article 2

This Law shall apply to any Person who commits legal acts as governed by this Law, both within jurisdiction of Indonesia and outside jurisdiction of Indonesia, having legal effect within jurisdiction of Indonesia and/or outside jurisdiction of Indonesia, and harms the interest of Indonesia.

Elucidation of Article 2:

Since Information Technology utilization for Electronic Information and Electronic Transactions is cross-territorial or universal in nature, this law has jurisdiction over legal acts applicable not only in Indonesia and/or committed by Indonesian citizens, but also applicable to legal acts committed outside jurisdiction of Indonesia by both Indonesian citizens and foreign citizens or Indonesian legal entities and foreign legal entities having legal effect in Indonesia.

"Harm the interest of Indonesia" includes but not limited to harm to the interests of national economy, strategic data protection, nation's dignity and degree, state defense and security, sovereignty, citizens as well as Indonesian legal entities.

CHAPTER II

PRINCIPLES AND OBJECTIVES

Article 3

Information Technology and Electronic Transaction shall be utilized under the principles of legal certainty, benefit, prudence, good faith, and freedom to choose technology or technology neutrality.

Elucidation of Article 3:

"Principle of legal certainty" means a legal foundation on which the utilization of Information Technology and Electronic Transaction as well as

mendukung penyelenggaraannya yang mendapatkan pengakuan hukum di dalam dan di luar pengadilan.

anything that supports its application are legally recognized inside and outside the court.

"Asas manfaat" berarti asas bagi pemanfaatan Teknologi Informasi dan Transaksi Elektronik diupayakan untuk mendukung proses berinformasi sehingga dapat meningkatkan kesejahteraan masyarakat.

"Principle of benefit" means a principle that Information Technology and Electronic Transaction are utilized to support the process of using information in order to enable improvement of public welfare.

"Asas kehati-hatian" berarti landasan bagi pihak yang bersangkutan harus memperhatikan segenap aspek yang berpotensi mendatangkan kerugian, baik bagi dirinya maupun pihak lain dalam pemanfaatan Teknologi Informasi dan Transaksi Elektronik.

"Principle of prudence" means a foundation on which the parties concerned must address themselves to any aspect with potential for causing damage to both himself/herself and other party in the utilization of Information Technology and Electronic Transactions.

"Asas iktikad baik" berarti asas yang digunakan para pihak dalam melakukan Transaksi Elektronik tidak bertujuan untuk secara sengaja dan tanpa hak atau melawan hukum mengakibatkan kerugian bagi pihak lain tanpa sepengetahuan pihak lain tersebut.

"Principle of good faith" means a principle that parties to an Electronic Transaction shall not intentionally, unauthorizedly or unlawfully aim at causing other parties any harm without the other parties' knowledge.

"Asas kebebasan memilih teknologi atau netral teknologi" berarti asas pemanfaatan Teknologi Informasi dan Transaksi Elektronik tidak terfokus pada penggunaan teknologi tertentu sehingga dapat mengikuti perkembangan pada masa yang akan datang.

"Principle of freedom to choose technology or technology neutrality" means a principle that, to keep abreast of the times, the utilization of Information Technology and Electronic Transactions is not focusing on the use of certain technology.

Pasal 4

Pemanfaatan Teknologi Informasi dan Transaksi Elektronik dilaksanakan dengan tujuan untuk:

a. mencerdaskan kehidupan bangsa sebagai bagian dari masyarakat informasi dunia;

b. mengembangkan perdagangan dan perekonomian nasional dalam rangka meningkatkan kesejahteraan masyarakat;

c. meningkatkan efektifitas dan efisiensi pelayanan publik;

d. membuka kesempatan seluas-luasnya kepada setiap Orang untuk memajukan pemikiran dan kemampuan di bidang penggunaan dan pemanfaatan Teknologi Informasi seoptimal mungkin dan bertanggung jawab; dan

e. memberikan rasa aman, keadilan, dan kepastian hukum bagi pengguna dan penyelenggara Teknologi Informasi.

Article 4

Information Technology and Electronic Transaction shall be utilized with the objectives:

a. to advance the intellectual life of the people as part of the world information community;

b. to develop the national trade and economy in order to improve public welfare;

c. to improve the effectiveness and efficiency of public services;

d. to give as wide opportunities as possible to any Person to cultivate his/her insight and capability in the optimal and responsible use and utilization of Information Technology; and

d. to give senses of security, justice, and legal certainty for Information Technology users and providers.

BAB III

INFORMASI, DOKUMEN, DAN TANDA TANGAN ELEKTRONIK

Pasal 5

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

Penjelasan Pasal 5 Ayat (1):

Bahwa keberadaan Informasi Elektronik dan/atau Dokumen Elektronik mengikat dan diakui sebagai alat bukti yang sah untuk memberikan kepastian hukum terhadap Penyelenggaraan Sistem Elektronik dan Transaksi Elektronik, terutama dalam pembuktian dan hal yang berkaitan dengan perbuatan hukum yang dilakukan melalui Sistem Elektronik.

(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.

Anotasi Pasal 5 ayat (1) dan ayat (2):

Menurut Putusan Mahkamah Konstitusi No. 20/PUU-XIV/2016, 7 September 2016, frasa "Informasi Elektronik dan/atau Dokumen Elektronik" bertentangan dengan UUD 1945 dan tidak mempunyai kekuatan hukum mengikat sepanjang tidak dimaknai khususnya frasa "Informasi Elektronik dan/atau Dokumen Elektronik" sebagai alat bukti dilakukan dalam rangka penegakan hukum atas permintaan kepolisian, kejaksaan, dan/atau institusi penegak hukum lainnya yang ditetapkan berdasarkan undang-undang sebagaimana ditentukan dalam Pasal 31 ayat (3).

Penjelasan Pasal 5 Ayat (2):

Khusus untuk Informasi Elektronik dan/atau Dokumen Elektronik berupa hasil intersepsi atau penyadapan atau perekaman yang merupakan bagian dari penyadapan harus dilakukan dalam rangka penegakan hukum atas permintaan kepolisian, kejaksaan, dan/atau institusi lainnya yang kewenangannya ditetapkan berdasarkan undang-undang.

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

CHAPTER III

ELECTRONIC INFORMATION, RECORDS, AND SIGNATURES

Article 5

(1) Electronic Information and/or Electronic Records and/or the printouts thereof shall be lawful means of proof.

Elucidation of Article 5 Section (1):

That the existence of Electronic Information and/or Electronic Records is binding and recognized as lawful means of proof in order to give legal certainty to the Provision of Electronic Systems and Electronic Transactions, especially in evidence and anything in connection with legal acts that are committed by means of Electronic Systems.

(2) Electronic Information and/or Electronic Records and/or the printouts thereof as referred to section (1) shall be the expanded lawful means of proof in accordance with the Law of Procedure prevailing in Indonesia.

Annotation of Article 5 section (1) and section (2):

Under Decision of the Constitutional Court No. 20/PUU-XIV/2016, September 7, 2016, the phrases "Electronic Information and/or Electronic Records" are against the 1945 Constitutional Law and have no binding force and effect of law, as long as the phrases, especially "Electronic Information and/or Electronic Records," are not meant to act as means of proof that is made in the scope of law enforcement at the request of the police, prosecutor's office, and/or other law enforcement institutions as provided by law under Article 31 section (3).

Elucidation of Article 5 Section (2):

Electronic Information and/or Electronic Records as a result of interception or wiretapping or recording as part of wiretapping must be made in the scope of law enforcement at the request of the police, prosecutor's office, and/or other institutions whose authority to do so is provided by law.

(3) Electronic Information and/or Electronic Records shall be declared to be lawful if using Electronic Systems in accordance with the provisions of this Law.

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

Penjelasan Pasal 5 Ayat (4) Huruf a:

Surat yang menurut undang-undang harus dibuat tertulis meliputi tetapi tidak terbatas pada surat berharga, surat yang berharga, dan surat yang digunakan dalam proses penegakan hukum acara perdata, pidana, dan administrasi negara.

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

Pasal 6

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.

Penjelasan Pasal 6:

Selama ini bentuk tertulis identik dengan informasi dan/atau dokumen yang tertuang di atas kertas semata, padahal pada hakikatnya informasi dan/atau dokumen dapat dituangkan ke dalam media apa saja, termasuk media elektronik. Dalam lingkup Sistem Elektronik, informasi yang asli dengan salinannya tidak relevan lagi untuk dibedakan sebab Sistem Elektronik pada dasarnya beroperasi dengan cara penggandaan yang mengakibatkan informasi yang asli tidak dapat dibedakan lagi dari salinannya.

Pasal 7

Setiap Orang yang menyatakan hak, memperkuat hak yang telah ada, atau menolak hak Orang lain berdasarkan adanya Informasi Elektronik dan/atau Dokumen Elektronik harus memastikan bahwa Informasi Elektronik dan/atau Dokumen Elektronik yang ada padanya berasal dari Sistem

(4) Provisions for Electronic Information and/or Electronic Records as referred to section (1) shall not apply to:

a. certificates that must by Law be made in a writing form; and

Elucidation of Article 5 Section (4) Point a:

Certificates that must by law be made in writing form shall include but not limited to negotiable instruments, valuable documents, and documents used in the process of law enforcement of civil procedure, criminal procedure, and state administration.

b. certificates along with their papers that must by Law be made in notarial deed or deed made by conveyancers.

Article 6

If there are other provisions other than those governed by Article 5 section (4) requiring that information must be in writing or original form, Electronic Information and/or Electronic Records shall be deemed to be lawful to the extent information contained therein is accessible, displayable, assured as to its integrity, and accountable in order to be explanatory.

Elucidation of Article 6:

Until the present, a writing form is identical to information and/or records contained on paper only when in fact information and/or records can essentially be inscribed on any medium, including electronic media. Within the context of Electronic Systems, it is no longer relevant to distinguish the original information from its copies because Electronic Systems can typically generate copies that make the original information can no longer be distinguished from them.

Article 7

Any Person who claims rights, affirms existing rights, or denies other Persons' rights with respect to the existence of Electronic Information and/or Electronic Records must ensure that Electronic Information and/or Electronic Records held by him/her originate in Electronic Systems eligible

Elektronik yang memenuhi syarat berdasarkan Peraturan Perundang-undangan.

Penjelasan Pasal 7:

Ketentuan ini dimaksudkan bahwa suatu Informasi Elektronik dan/atau Dokumen Elektronik dapat digunakan sebagai alasan timbulnya suatu hak.

Pasal 8

(1) Kecuali diperjanjikan lain, waktu pengiriman suatu Informasi Elektronik dan/atau Dokumen Elektronik ditentukan pada saat Informasi Elektronik dan/atau Dokumen Elektronik telah dikirim dengan alamat yang benar oleh Pengirim ke suatu Sistem Elektronik yang ditunjuk atau dipergunakan Penerima dan telah memasuki Sistem Elektronik yang berada di luar kendali Pengirim.

(2) Kecuali diperjanjikan lain, waktu penerimaan suatu Informasi Elektronik dan/atau Dokumen Elektronik ditentukan pada saat Informasi Elektronik dan/atau Dokumen Elektronik memasuki Sistem Elektronik di bawah kendali Penerima yang berhak.

(3) Dalam hal Penerima telah menunjuk suatu Sistem Elektronik tertentu untuk menerima Informasi Elektronik, penerimaan terjadi pada saat Informasi Elektronik dan/atau Dokumen Elektronik memasuki Sistem Elektronik yang ditunjuk.

(4) Dalam hal terdapat dua atau lebih sistem informasi yang digunakan dalam pengiriman atau penerimaan Informasi Elektronik dan/atau Dokumen Elektronik, maka:

a. waktu pengiriman adalah ketika Informasi Elektronik dan/atau Dokumen Elektronik memasuki sistem informasi pertama yang berada di luar kendali Pengirim.

b. waktu penerimaan adalah ketika Informasi Elektronik dan/atau Dokumen Elektronik memasuki sistem informasi terakhir yang berada di bawah kendali Penerima.

Pasal 9

Pelaku usaha yang menawarkan produk melalui

under the Laws and Regulations.

Elucidation of Article 7:

This provision means that Electronic Information and/or Electronic Records may be used as grounds from which rights accrue.

Article 8

(1) Unless agreed otherwise, time of sending of Electronic Information and/or Electronic Records shall be timed when the Electronic Information and/or Electronic Records are sent to the proper address by the Senders/Originators to Electronic Systems the Recipients/Addressees designate or use, and have entered Electronic Systems beyond the control of the Senders/Originators.

(2) Unless agreed otherwise, the time of receipt of Electronic Information and/or Electronic Records shall be timed when the Electronic Information and/or Electronic Records enter Electronic Systems under the control of the authorized Recipients/Addressees.

(3) If Recipients/Addressees have designated specific Electronic Systems to receive Electronic Information, reception shall occur when Electronic Information and/or Electronic Records enter designated Electronic Systems.

(4) If there are two or more information systems used in the sending or reception of Electronic Information and/or Electronic Records, then:

a. the time of sending shall be the time when Electronic Information and/or Electronic Records enter a first information system beyond the control of the Senders/ Originators.

b. the time of receipt shall be the time when Electronic Information and/or Electronic Records enter a last information system under the control of the Recipients/Addressees.

Article 9

Business actors that offer products by means of

Sistem Elektronik harus menyediakan informasi yang lengkap dan benar berkaitan dengan syarat kontrak, produsen, dan produk yang ditawarkan.

Penjelasan Pasal 9:

Yang dimaksud dengan "informasi yang lengkap dan benar" meliputi:

a. Informasi yang memuat identitas serta status subjek hukum dan kompetensinya, baik sebagai produsen, pemasok, penyelenggara maupun perantara;

b. Informasi lain yang menjelaskan hal tertentu yang menjadi syarat sahnya perjanjian serta menjelaskan barang dan/atau jasa yang ditawarkan, seperti nama, alamat, dan deskripsi barang/jasa.

Pasal 10

(1) Setiap pelaku usaha yang menyelenggarakan Transaksi Elektronik dapat disertifikasi oleh Lembaga Sertifikasi Keandalan.

Penjelasan Pasal 10 Ayat (1):

Sertifikasi Keandalan dimaksudkan sebagai bukti bahwa pelaku usaha yang melakukan perdagangan secara elektronik layak berusaha setelah melalui penilaian dan audit dari badan yang berwenang. Bukti telah dilakukan Sertifikasi Keandalan ditunjukkan dengan adanya logo sertifikasi berupa trust mark pada laman (home page) pelaku usaha tersebut.

(2) Ketentuan mengenai pembentukan Lembaga Sertifikasi Keandalan sebagaimana dimaksud dalam ayat (1) diatur dengan Peraturan Pemerintah.

Pasal 11

(1) Tanda Tangan Elektronik memiliki kekuatan hukum dan akibat hukum yang sah selama memenuhi persyaratan sebagai berikut:

a. data pembuatan Tanda Tangan Elektronik terkait hanya kepada Penanda Tangan;

b. data pembuatan Tanda Tangan Elektronik pada saat proses penandatanganan elektronik hanya berada dalam kuasa Penanda Tangan;

c. Segala perubahan terhadap Tanda Tangan

Electronic Systems must make available full and true information about contractual conditions, producers, and products offered.

Elucidation of Article 9:

"Full and true information" includes:

a. Information that contains identity as well as status of legal subjects and their competency, whether as producers, suppliers, providers or intermediaries;

b. Other information that explains specific matters of requirements for validity of agreements, as well as explains goods and/or services offered, such as names, addresses, and descriptions of goods/services.

Article 10

(1) Any business actor who conducts Electronic Transactions may be certified by a Trustworthiness Certification Institution.

Elucidation of Article 10 section (1):

Trustworthiness Certification serves as proof that business actors who conduct trade electronically are eligible to do business upon assessment and audits by a competent body. Proof that Trustworthiness Certification has been made shall be demonstrated by a trustmark certification logo on the homepage of the business actor.

(2) Provisions for formation of a Trustworthiness Certification Institution as referred to in section (1) shall be governed by Regulation of the Government.

Article 11

(1) Electronic Signatures shall have lawful force and legal effect of law if satisfying the following requirements:

a. Electronic Signature-creation data shall be associated only with the Signatories/ Signers;

b. Electronic Signature-creation data shall, during the electronic signing process, be in the possession of the Signatories/ Signers only;

c. Any alteration in Electronic Signatures

Elektronik yang terjadi setelah waktu penandatanganan dapat diketahui;

d. Segala perubahan terhadap Informasi Elektronik yang terkait dengan Tanda Tangan Elektronik tersebut setelah waktu penandatanganan dapat diketahui;

e. Terdapat cara tertentu yang dipakai untuk mengidentifikasi siapa Penandatangannya; dan

f. Terdapat cara tertentu untuk menunjukkan bahwa Penanda Tangan telah memberikan persetujuan terhadap Informasi Elektronik yang terkait.

Penjelasan Pasal 11 Ayat (1):

Undang-Undang ini memberikan pengakuan secara tegas bahwa meskipun hanya merupakan suatu kode, Tanda Tangan Elektronik memiliki kedudukan yang sama dengan tanda tangan manual pada umumnya yang memiliki kekuatan hukum dan akibat hukum.

Persyaratan sebagaimana dimaksud dalam Pasal ini merupakan persyaratan minimum yang harus dipenuhi dalam setiap Tanda Tangan Elektronik. Ketentuan ini membuka kesempatan seluas-luasnya kepada siapapun untuk mengembangkan metode, teknik, atau proses pembuatan Tanda Tangan Elektronik.

(2) Ketentuan lebih lanjut mengenai Tanda Tangan Elektronik sebagaimana dimaksud pada ayat (1) diatur dengan Peraturan Pemerintah.

Penjelasan Pasal 11 Ayat (2):

Peraturan Pemerintah dimaksud, antara lain, mengatur tentang teknik, metode, sarana, dan proses pembuatan Tanda Tangan Elektronik.

Pasal 12

(1) Setiap Orang yang terlibat dalam Tanda Tangan Elektronik berkewajiban memberikan pengamanan atas Tanda Tangan Elektronik yang digunakannya;

(2) Pengamanan Tanda Tangan Elektronik sebagaimana dimaksud pada ayat (1) sekurang-kurangnya meliputi:

a. sistem tidak dapat diakses oleh Orang

that occur after the signing time is knowable;

d. Any alteration in Electronic Information associated with the Electronic Signatures after the signing time is knowable;

e. There are certain methods adopted to identify the identity of the Signatories/ Signers; and

f. There are certain methods to demonstrate that the Signatories/Signers have given consent to the associated Electronic Information;

Elucidation of Article 11 Section (1):

This Law grants recognition definitely that despite codes, Electronic Signatures have an equal position to manual signatures in general, with force and legal effect of law.

The requirements as referred to in this Article are the minimum requirements that must be satisfied by any Electronic Signature. This provision allows anyone as wide opportunities as possible to develop methods, techniques, or process to create Electronic Signatures.

(2) Ancillary provisions for Electronic Signatures as referred to in section (1) shall be governed by Regulation of the Government.

Elucidation of Article 11 Section (2):

The Regulation of the Government concerned governs, inter alia, techniques, methods, means or process to create Electronic Signatures.

Article 12

(1) Any Person who is involved in electronic signing shall be required to provide security of the Electronic Signatures he/she uses;

(2) Security of Electronic Signatures as referred to in section (1) shall include at least:

a. the systems are not accessible to

lain yang tidak berhak;

b. Penanda Tangan harus menerapkan prinsip kehati-hatian untuk menghindari penggunaan secara tidak sah terhadap data terkait pembuatan Tanda Tangan Elektronik;

c. Penanda Tangan harus tanpa menunda-nunda, menggunakan cara yang dianjurkan oleh penyelenggara Tanda Tangan Elektronik ataupun cara lain yang layak dan sepatutnya harus segera memberitahukan kepada seseorang yang oleh Penanda Tangan dianggap memercayai Tanda Tangan Elektronik atau kepada pihak pendukung layanan Tanda Tangan Elektronik jika:

1. Penanda Tangan mengetahui bahwa data pembuatan Tanda Tangan Elektronik telah dibobol; atau

2. keadaan yang diketahui oleh Penanda Tangan dapat menimbulkan risiko yang berarti, kemungkinan akibat bobolnya data pembuatan Tanda Tangan Elektronik; dan

d. dalam hal Sertifikat Elektronik digunakan untuk mendukung Tanda Tangan Elektronik, Penanda Tangan harus memastikan kebenaran dan keutuhan semua informasi yang terkait dengan Sertifikat Elektronik tersebut.

(3) Setiap Orang yang melakukan pelanggaran ketentuan sebagaimana dimaksud pada ayat (1), bertanggung jawab atas segala kerugian dan konsekuensi hukum yang timbul.

BAB IV

PENYELENGGARAAN SERTIFIKASI ELEKTRONIK DAN SISTEM ELEKTRONIK

Bagian Kesatu

Penyelenggaraan Sertifikasi Elektronik

Pasal 13

(1) Setiap Orang berhak menggunakan jasa Penyelenggara Sertifikasi Elektronik untuk pembuatan Tanda Tangan Elektronik.

unauthorized Persons;

b. the Signatories/Signers must apply the principle of prudence to avoid unauthorized uses of Electronic Signature-creation data;

c. the Signatories/Signers must without delay adopt methods recommended by Electronic Signature providers, or other appropriate methods, and must promptly notify Persons whom the Signatories/Signers consider to be relying on the Electronic Signatures, or notify parties that support Electronic Signature services if:

1. the Signatories/Signers know that the Electronic Signature-creation data has been compromised; or

2. circumstances known to the Signatories/Signers may pose considerable risks due likely to the Electronic Signature-creation data being compromised; and

d. if Electronic Certificates are used to support Electronic Signatures, the Signatories/Signers must confirm the truth and integrity of all information in connection with the Electronic Certificates.

(3) Any Person who violates the provisions of section (1) shall be liable for any damage and legal consequence resulting therefrom.

CHAPTER IV

PROVISION OF ELECTRONIC CERTIFICATION AND ELECTRONIC SYSTEMS

Part One

Provision of Electronic Certification

Article 13

(1) Any Person shall be entitled to engage the service of Electronic Certification Service Providers to create Electronic Signatures.

(2) Penyelenggara Sertifikasi Elektronik harus memastikan keterkaitan suatu Tanda Tangan Elektronik dengan pemiliknya.

(3) Penyelenggara Sertifikasi Elektronik terdiri atas:

a. Penyelenggara Sertifikasi Elektronik Indonesia; dan

b. Penyelenggara Sertifikasi Elektronik asing.

(4) Penyelenggara Sertifikasi Elektronik Indonesia berbadan hukum Indonesia dan berdomisili di Indonesia.

(5) Penyelenggara Sertifikasi Elektronik asing yang beroperasi di Indonesia harus terdaftar di Indonesia.

(6) Ketentuan lebih lanjut mengenai Penyelenggara Sertifikasi Elektronik sebagaimana dimaksud pada ayat (3) diatur dengan Peraturan Pemerintah.

Pasal 14

Penyelenggara Sertifikasi Elektronik sebagaimana dimaksud pada Pasal 13 ayat (1) sampai dengan ayat (5) harus menyediakan informasi yang akurat, jelas, dan pasti kepada setiap pengguna jasa, yang meliputi:

a. metode yang digunakan untuk mengidentifikasi Penanda Tangan;

b. hal yang dapat digunakan untuk mengetahui data diri pembuatan Tanda Tangan Elektronik;

c. hal yang dapat menunjukkan keberlakuan dan keamanan Tanda Tangan Elektronik;

Penjelasan Pasal 14:

Informasi sebagaimana dimaksud dalam Pasal ini adalah informasi yang minimum harus dipenuhi oleh setiap penyelenggara Tanda Tangan Elektronik.

Bagian Kedua

Penyelenggaraan Sistem Elektronik

Pasal 15

(1) Setiap Penyelenggara Sistem Elektronik harus

(2) Electronic Certification Service Providers must confirm the attribution of an Electronic Signature to the owner.

(3) Electronic Certification Service Providers shall include:

a. Indonesian Electronic Certification Service Providers; and

b. foreign Electronic Certification Service Providers.

(4) Indonesian Electronic Certification Service Providers shall be an Indonesian legal entity and domiciled in Indonesia.

(5) Foreign Electronic Certification Service Providers that operate in Indonesia must be registered in Indonesia.

(6) Ancillary provisions for Electronic Certification Service Providers as referred to in section (3) shall be governed by Regulation of the Government.

Article 14

Electronic Certification Service Providers as referred to in Article 13 section (1) through section (5) must make available to any service user accurate, clear, and definite information that includes:

a. methods that are adopted to identify the Signatories/Signers;

b. things that can be used to recognize Electronic Signature-creation personal data;

c. things that can demonstrate the validity and security of Electronic Signatures;

Elucidation of Article 14:

Information as referred to in this Article is the minimum information that must be satisfied by every Electronic Signature service provider.

Part Two

Provision of Electronic Systems

Article 15

(1) Any Electronic System Provider must provide

menyelenggarakan Sistem Elektronik secara andal dan aman serta bertanggung jawab terhadap beroperasinya Sistem Elektronik sebagaimana mestinya.

Penjelasan Pasal 15 Ayat (1):

"Andal" artinya Sistem Elektronik memiliki kemampuan yang sesuai dengan kebutuhan penggunaannya.

"Aman" artinya Sistem Elektronik terlindungi secara fisik dan nonfisik.

"Beroperasi sebagaimana mestinya" artinya Sistem Elektronik memiliki kemampuan sesuai dengan spesifikasinya.

(2) Penyelenggara Sistem Elektronik bertanggung jawab terhadap Penyelenggaraan Sistem Elektroniknya.

Penjelasan Pasal 15 Ayat (2):

"Bertanggung jawab" artinya ada subjek hukum yang bertanggung jawab secara hukum terhadap Penyelenggaraan Sistem Elektronik tersebut.

(3) Ketentuan sebagaimana dimaksud pada ayat (2) tidak berlaku dalam hal dapat dibuktikan terjadinya keadaan memaksa, kesalahan, dan/atau kelalaian pihak pengguna Sistem Elektronik.

Pasal 16

(1) Sepanjang tidak ditentukan lain oleh undang-undang tersendiri, setiap Penyelenggara Sistem Elektronik wajib mengoperasikan Sistem Elektronik yang memenuhi persyaratan minimum sebagai berikut:

a. dapat menampilkan kembali Informasi Elektronik dan/atau Dokumen Elektronik secara utuh sesuai dengan masa retensi yang ditetapkan dengan Peraturan Perundang-undangan;

b. dapat melindungi ketersediaan, keutuhan, keotentikan, kerahasiaan, dan keteraksesan, Informasi Elektronik dalam Penyelenggaraan Sistem Elektronik tersebut;

c. dapat beroperasi sesuai dengan prosedur atau petunjuk dalam Penyelenggaraan Sistem Elektronik tersebut;

Electronic Systems in reliable and secure manner and shall be responsible for the proper operation of the Electronic Systems.

Elucidation of Article 15 Section (1):

"Reliable" means the Electronic Systems have the capabilities that match the needs of the users.

"Secure" means the Electronic Systems are protected in a physical and non-physical manner.

"Proper operation" means the Electronic Systems have the capabilities that match their specifications.

(2) Electronic System providers shall be liable for their Provision of Electronic Systems.

Elucidation of Article 15 Section (2):

"Liable" means there is a legal subject that is legally responsible (liable) for such Provision of Electronic Systems.

(3) The provision of section (2) shall not apply if it is verifiable that there occur compelling circumstances, fault, and/or negligence on the part of the Electronic System users.

Article 16

(1) To the extent not provided otherwise by individual laws, any Electronic System Providers shall be required to operate Electronic Systems in compliance with the following minimum requirements:

a. able to redisplay Electronic Information and/or Electronic Records in their entirety in accordance with the retention period as provided for by the Laws and Regulations;

b. able to protect the availability, integrity, authenticity, confidentiality, and accessibility of Electronic Information in the provision of Electronic Systems;

c. able to operate in compliance with the procedures or guidelines for the provision of Electronic Systems;

d. dilengkapi dengan prosedur atau petunjuk yang diumumkan dengan bahasa, informasi, atau simbol yang dapat dipahami oleh pihak yang bersangkutan dengan Penyelenggaraan Sistem Elektronik tersebut; dan

e. memiliki mekanisme yang berkelanjutan untuk menjaga kebaruan, kejelasan, dan kebertanggungjawaban prosedur atau petunjuk;

(2) Ketentuan lebih lanjut tentang Penyelenggaraan Sistem Elektronik sebagaimana dimaksud pada ayat (1) diatur dengan Peraturan Pemerintah.

BAB V

TRANSAKSI ELEKTRONIK

Pasal 17

(1) Penyelenggaraan Transaksi Elektronik dapat dilakukan dalam lingkup publik atau privat.

Penjelasan Pasal 17 Ayat (1):

Undang-Undang ini memberikan peluang terhadap pemanfaatan Teknologi Informasi oleh penyelenggara negara, Orang, Badan Usaha, dan/atau masyarakat.

Pemanfaatan Teknologi Informasi harus dilakukan secara baik, bijaksana, bertanggung jawab, efektif, dan efisien agar dapat diperoleh manfaat yang sebesar-besarnya bagi masyarakat.

(2) Para pihak yang melakukan Transaksi Elektronik sebagaimana dimaksud pada ayat (1) wajib beriktikad baik dalam melakukan interaksi dan/atau pertukaran Informasi Elektronik dan/atau Dokumen Elektronik selama transaksi berlangsung.

(3) Ketentuan lebih lanjut mengenai penyelenggaraan Transaksi Elektronik sebagaimana dimaksud pada ayat (1) diatur dengan Peraturan Pemerintah.

Pasal 18

(1) Transaksi Elektronik yang dituangkan ke dalam Kontrak Elektronik mengikat para pihak.

(2) Para pihak memiliki kewenangan untuk

d. accompanied by the procedures or guidelines that are announced in languages, information, or symbols that are intelligible to parties attributed to the provision of Electronic Systems; and

e. adopt sustainable mechanism in order to maintain updates, clarity, and accountability for the procedures or guidelines;

(2) Ancillary provisions for provision of Electronic Systems as referred to in section (1) shall be governed by Regulation of the Government.

CHAPTER V

ELECTRONIC TRANSACTIONS

Article 17

(1) Electronic Transactions may be provided by the public or private sector.

Elucidation of Article 17 Section (1):

This Law allows state administrators, Persons, Business Entities, and/or the public opportunities to utilize Information Technology.

Information Technology must be utilized in a proper, responsible, effective, and efficient manner for the public to reap as much benefits as possible.

(2) Parties that conduct Electronic Transactions as referred to in section (1) must, during the transactions, be in good faith in making interaction and/or exchange of Electronic Information and/or Electronic Records.

(3) Ancillary provisions for provision of Electronic Transactions as referred to in section (1) shall be governed by Regulation of the Government.

Article 18

(1) Electronic Transactions that are stated in Electronic Contracts shall bind on parties.

(2) Parties shall have discretion to choose law

memilih hukum yang berlaku bagi Transaksi Elektronik internasional yang dibuatnya.

Penjelasan Pasal 18 Ayat (2):

Pilihan hukum yang dilakukan oleh para pihak dalam kontrak internasional termasuk yang dilakukan secara elektronik dikenal dengan choice of law. *Hukum ini mengikat sebagai hukum yang berlaku bagi kontrak tersebut.*

Pilihan hukum dalam Transaksi Elektronik hanya dapat dilakukan jika dalam kontraknya terdapat unsur asing dan penerapannya harus sejalan dengan prinsip-prinsip hukum perdata internasional (HPI).

(3) Jika para pihak tidak melakukan pilihan hukum dalam Transaksi Elektronik internasional, hukum yang berlaku didasarkan pada asas Hukum Perdata Internasional.

Penjelasan Pasal 18 Ayat (3):

Dalam hal tidak ada pilihan hukum, penetapan hukum yang berlaku berdasarkan prinsip atau asas hukum perdata internasional yang akan ditetapkan sebagai hukum yang berlaku pada kontrak tersebut.

(4) Para pihak memiliki kewenangan untuk menetapkan forum pengadilan, arbitrase, atau lembaga penyelesaian sengketa alternatif lainnya yang berwenang menangani sengketa yang mungkin timbul dari Transaksi Elektronik internasional yang dibuatnya.

Penjelasan Pasal 18 Ayat (4):

Forum yang berwenang mengadili sengketa kontrak internasional, termasuk yang dilakukan secara elektronik, adalah forum yang dipilih oleh para pihak. Forum tersebut dapat berbentuk pengadilan, arbitrase, atau lembaga penyelesaian sengketa alternatif lainnya.

(5) Jika para pihak tidak melakukan pilihan forum sebagaimana dimaksud pada ayat (4), penetapan kewenangan pengadilan, arbitrase, atau lembaga penyelesaian sengketa alternatif lainnya yang berwenang menangani sengketa yang mungkin timbul dari transaksi tersebut, didasarkan pada asas Hukum Perdata Internasional.

Penjelasan Pasal 18 Ayat (5):

Dalam hal para pihak tidak melakukan pilihan forum, kewenangan forum berlaku berdasarkan

applicable to the international Electronic Transactions they enter.

Elucidation of Article 18 Section (2):

Pilihan hukum *made by parties in the international contracts, including electronically-made contracts, is known as choice of law. This law binds as law that applies to such contracts.*

Choice of law in Electronic Transactions may be made only if the contracts contain foreign elements, and their applicability must be in harmony with the principles of the private international law.

(3) If no parties make choice of law in the international Electronic Transactions, the applicable law shall refer to the principles of the Private International Law.

Elucidation of Article 18 Section (3):

If there is no choice of law, the law held applicable to the contracts shall be the principles or tenets of the private international law.

(4) Parties shall have discretion to determine forums of court, arbitration, or other alternative dispute resolution tribunals with jurisdiction to handle disputes that may arise from the international Electronic Transactions they enter.

Elucidation of Article 18 Section (4):

Forums with jurisdiction to adjudicate international contract disputes, including electronically-made contracts, shall be forums chosen by parties. Such forums may be in the form of court, arbitration, or other alternative dispute resolution tribunal.

(5) If no parties make choice of forum as referred to in section (4), the jurisdiction of court, arbitration, or other alternative dispute resolution tribunal with jurisdiction to handle disputes that may arise from such transactions shall be determined under the principles of the Private International Law.

Elucidation of Article 18 Section (5):

If no parties make choice of forum, jurisdiction of forum under the principles of the Private

*prinsip atau asas hukum perdata internasional. Asas tersebut dikenal dengan asas tempat tinggal tergugat (*the basis of presence*) dan efektivitas yang menekankan pada tempat harta harta tergugat berada (*principle of effectiveness*).*

International Law shall apply. Such principles are known as the principle of the residence of the defendants (the basis of presence) and the principle of effectiveness that emphasizes the place of assets of the defendants (principle of effectiveness).

Pasal 19

Para pihak yang melakukan Transaksi Elektronik harus menggunakan Sistem Elektronik yang disepakati.

Article 19

Parties that conduct Electronic Transactions must adopt agreed-on Electronic Systems.

Penjelasan Pasal 19:

Yang dimaksud dengan "disepakati" dalam pasal ini juga mencakup disepakatinya prosedur yang terdapat dalam Sistem Elektronik yang bersangkutan.

Elucidation of Article 19:

"Agreed-on" in this article also includes agreeing with the procedures contained in the Electronic Systems concerned.

Pasal 20

(1) Kecuali ditentukan lain oleh para pihak, Transaksi Elektronik terjadi pada saat penawaran transaksi yang dikirim Pengirim telah diterima dan disetujui Penerima.

Article 20

(1) Unless provided otherwise by parties, Electronic Transactions shall occur when the transaction offers sent by Senders/Originators have been received and accepted by the Recipients/Addressees.

Penjelasan Pasal 20 Ayat (1):

*Transaksi Elektronik terjadi pada saat kesepakatan antara para pihak yang dapat berupa, antara lain pengecekan data, identitas, nomor identifikasi pribadi (*personal identification number/PIN*) atau sandi lewat (*password*).*

Elucidation of Article 20 Section (1):

An electronic Transaction takes place when the parties have reached an agreement, such as, inter alia, verification of data, identity, personal identification number/PIN or password.

(2) Persetujuan atas penawaran Transaksi Elektronik sebagaimana dimaksud pada ayat (1) harus dilakukan dengan pernyataan penerimaan secara elektronik.

(2) Acceptance on the Electronic Transaction offers as referred to in section (1) must be made with an electronic acknowledgement of its receipt.

Pasal 21

(1) Pengirim atau Penerima dapat melakukan Transaksi Elektronik sendiri, melalui pihak yang dikuasakan olehnya, atau melalui Agen Elektronik.

Article 21

(1) Senders/Originators or Recipients/Addressees may conduct Electronic Transactions in person, or by his/her authorized persons, or by Electronic Agents.

Penjelasan Pasal 21 Ayat (1):

Yang dimaksud dengan "dikuasakan" dalam ketentuan ini sebaiknya dinyatakan dalam surat kuasa.

Elucidation of Article 21 Section (1):

It is advisable to "authorize a person" by virtue of a power of attorney.

(2) Pihak yang bertanggung jawab atas segala akibat hukum dalam pelaksanaan Transaksi Elektronik sebagaimana dimaksud pada ayat (1) diatur sebagai berikut:

(2) The extent to which Parties are liable for any legal effect in the conduct of Electronic Transactions as referred to in section (1) shall be governed as follows:

a. jika dilakukan sendiri, segala akibat hukum dalam pelaksanaan Transaksi Elektronik menjadi tanggung jawab para pihak yang bertransaksi;

b. jika dilakukan melalui pemberian kuasa, segala akibat hukum dalam pelaksanaan Transaksi Elektronik menjadi tanggung jawab pemberi kuasa; atau

c. jika dilakukan melalui Agen Elektronik, segala akibat hukum dalam pelaksanaan Transaksi Elektronik menjadi tanggung jawab penyelenggara Agen Elektronik.

(3) Jika kerugian Transaksi Elektronik disebabkan gagal beroperasinya Agen Elektronik akibat tindakan pihak ketiga secara langsung terhadap Sistem Elektronik, segala akibat hukum menjadi tanggung jawab penyelenggara Agen Elektronik.

(4) Jika kerugian Transaksi Elektronik disebabkan gagal beroperasinya Agen Elektronik akibat kelalaian pihak pengguna jasa layanan, segala akibat hukum menjadi tanggung jawab pengguna jasa layanan.

(5) Ketentuan sebagaimana dimaksud pada ayat (2) tidak berlaku dalam hal dapat dibuktikan terjadinya keadaan memaksa, kesalahan, dan/atau kelalaian pihak pengguna Sistem Elektronik.

Pasal 22

(1) Penyelenggara Agen Elektronik tertentu harus menyediakan fitur pada Agen Elektronik yang dioperasikannya yang memungkinkan penggunanya melakukan perubahan informasi yang masih dalam proses transaksi.

Penjelasan Pasal Pasal 22 Ayat (1):

Yang dimaksud dengan "fitur" adalah fasilitas yang memberikan kesempatan kepada pengguna Agen Elektronik untuk melakukan perubahan atas informasi yang disampaikannya, misalnya fasilitas pembatalan (cancel), edit, dan konfirmasi ulang.

(2) Ketentuan lebih lanjut mengenai penyelenggara Agen Elektronik tertentu sebagaimana dimaksud pada ayat (1) diatur dengan Peraturan Pemerintah.

a. if conducted in person, any legal effect in the conduct of Electronic Transactions shall be the liability of the parties to a transaction;

b. if conducted by an authorized person, any legal effect in the conduct of Electronic Transactions shall be the liability of the grantors; or

c. if conducted by Electronic Agents, any legal effect in the conduct of Electronic Transactions shall be the liability of the Electronic Agents.

(3) If harm to Electronic Transactions is caused by non-operation of Electronic Agents due to third parties' direct measures against Electronic Systems, any legal effect shall be the liability of the Electronic Agents.

(4) If harm to Electronic Transactions is caused by non-operation of Electronic Agents due to negligence of the service users, any legal effect shall be the liability of the service users.

(5) The provision of section (2) shall not apply if provable that there occur compelling circumstances, fault and/or negligence on the part of the Electronic System users.

Article 22

(1) Certain Electronic Agent Providers must provide features to Electronic Agents they operate to enable their users to alter information pending the process of transaction.

Elucidation of Article 22 Section (1):

"Features" means facilities that are provided for Electronic Agent users to alter information conveyed to them, for example, facilities such as cancel, edit, and reconfirm.

(2) Ancillary provisions for certain Electronic Agent providers as referred to in section (1) shall be governed by Regulation of the Government.

BAB VI

NAMA DOMAIN, HAK KEKAYAAN INTELEKTUAL, DAN PERLINDUNGAN HAK PRIBADI

Pasal 23

(1) Setiap penyelenggara negara, Orang, Badan Usaha, dan/atau masyarakat berhak memiliki Nama Domain berdasarkan prinsip pendaftar pertama.

Penjelasan Pasal 23 Ayat (1):

Nama Domain berupa alamat atau jati diri penyelenggara negara, Orang, Badan Usaha, dan/atau masyarakat, yang perolehannya didasarkan pada prinsip pendaftar pertama (first come first serve).

Prinsip pendaftar pertama berbeda antara ketentuan dalam Nama Domain dan dalam bidang hak kekayaan intelektual karena tidak diperlukan pemeriksaan substantif, seperti pemeriksaan dalam pendaftaran merek dan paten.

(2) Pemilikan dan penggunaan Nama Domain sebagaimana dimaksud pada ayat (1) harus didasarkan pada iktikad baik, tidak melanggar prinsip persaingan usaha secara sehat, dan tidak melanggar hak Orang lain.

Penjelasan Pasal 23 Ayat (2):

Yang dimaksud dengan "melanggar hak Orang lain", misalnya melanggar merek terdaftar, nama badan hukum terdaftar, nama Orang terkenal, dan sejenisnya yang pada intinya merugikan Orang lain.

(3) Setiap penyelenggara negara, Orang, Badan Usaha, atau masyarakat yang dirugikan karena penggunaan Nama Domain secara tanpa hak oleh Orang lain, berhak mengajukan gugatan pembatalan Nama Domain dimaksud.

Penjelasan Pasal 23 Ayat (3):

Yang dimaksud dengan "penggunaan Nama Domain secara tanpa hak" adalah pendaftaran dan penggunaan Nama Domain yang semata-mata ditujukan untuk menghalangi atau menghambat Orang lain untuk menggunakan nama yang intuitif dengan keberadaan nama dirinya atau nama produknya, atau untuk mendompleng reputasi Orang yang sudah terkenal atau ternama, atau untuk menyesatkan

CHAPTER VI

DOMAIN NAMES, INTELLECTUAL PROPERTY RIGHTS AND PROTECTION OF PRIVACY RIGHTS

Article 23

(1) Any state administrator, Person, Business Entity, and/or the public shall be entitled to hold Domain Names on a first applicant principle basis.

Elucidation of Article 23 Section (1):

Domain Names shall be addresses or identity of state administrators, Persons, Business Entities and/or the public obtained on a first applicant principle basis (first come, first served).

The first applicant principle in Domain Name policy is distinct from one in the field of Intellectual Property Rights in that no substantive examination is required when it is the case in the registration of trademarks and patents.

(2) Domain Names as referred to in section (1) must be held and used in good faith, non-violation of fair business competition, and non-infringement of the rights of other Persons.

Elucidation of Article 23 Section (2):

"Infringement of the rights of other Persons" means, for example, infringement of registered trademarks, registered names of legal entities, names of famous Persons, and the like, that substantially harm other Persons.

(3) Any state administrator, Person, Business Entity, or the public harmed by other Persons' unauthorized use of Domain Names shall be entitled to file a petition to cancel such Domain Names.

Elucidation of Article 23 Section (3):

"Unauthorized use of Domain Names" means the registration and use of Domain Names only aim at inhibiting or preventing other Persons from using a name which is intuitively their proper name or product names, or cashing in on the reputation of famous or well-known Persons, or misleading consumers.

konsumen.

Pasal 24

(1) Pengelola Nama Domain adalah Pemerintah dan/atau masyarakat.

(2) Dalam hal terjadi perselisihan pengelolaan Nama Domain oleh masyarakat, Pemerintah berhak mengambil alih sementara pengelolaan Nama Domain yang diperselisihkan.

(3) Pengelola Nama Domain yang berada di luar wilayah Indonesia dan Nama Domain yang diregistrasinya diakui keberadaannya sepanjang tidak bertentangan dengan Peraturan Perundang-undangan.

(4) Ketentuan lebih lanjut mengenai pengelolaan Nama Domain sebagaimana dimaksud pada ayat (1), ayat (2), dan ayat (3) diatur dengan Peraturan Pemerintah.

Pasal 25

Informasi Elektronik dan/atau Dokumen Elektronik yang disusun menjadi karya intelektual, situs internet, dan karya intelektual yang ada di dalamnya dilindungi sebagai Hak Kekayaan Intelektual berdasarkan ketentuan Peraturan Perundang-undangan.

Penjelasan Pasal 25:

Informasi Elektronik dan/atau Dokumen Elektronik yang disusun dan didaftarkan sebagai karya intelektual, hak cipta, paten, merek, rahasia dagang, desain industri, dan sejenisnya wajib dilindungi oleh Undang-Undang ini dengan memperhatikan ketentuan Peraturan Perundang-undangan.

Pasal 26

(1) Kecuali ditentukan lain oleh Peraturan Perundang-undangan, penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan Orang yang bersangkutan.

Penjelasan Pasal 26 Ayat (1):

*Dalam pemanfaatan Teknologi Informasi, perlindungan data pribadi merupakan salah satu bagian dari hak pribadi (*privacy rights*). Hak pribadi mengandung pengertian sebagai berikut:*

Article 24

(1) The Government and/or the public shall be the Domain Name administrators.

(2) If a dispute on Domain Name administration by the public arises, the Government shall be entitled to temporarily take over the Domain Name administration in dispute.

(3) Domain Name administrators residing outside the territory of Indonesia and Domain Names they have registered shall be recognized as to its existence to the extent not against the Laws and Regulations.

(4) Ancillary provisions for Domain Name administration as referred to in section (1), section (2), and section (3) shall be governed by Regulation of the Government.

Article 25

Electronic Information and/or Electronic Records that are created into intellectual works, internet sites, and intellectual works contained therein shall be protected as Intellectual Property Rights by the Laws and Regulations.

Elucidation of Article 25:

Electronic Information and/or Electronic Records created into and registered as intellectual works, copyrights, patents, trademarks, trade secret, industrial designs, and the like must be protected by this Law with due regard to the laws and regulations.

Article 26

(1) Unless provided otherwise by Laws and Regulations, use of any information through electronic media that involves personal data of a Person must be made by consent of the Person concerned.

Elucidation of Article 26 Section (1):

In the utilization of Information Technology, personal data belong to one of the privacy rights subject to protection. Privacy rights include the following meaning:

a. *Hak pribadi merupakan hak untuk menikmati kehidupan pribadi dan bebas dari segala macam gangguan.*

b. *Hak pribadi merupakan hak untuk dapat berkomunikasi dengan Orang lain tanpa tindakan memata-matai.*

c. *Hak pribadi merupakan hak untuk mengawasi akses informasi tentang kehidupan pribadi dan data seseorang.*

(2) Setiap Orang yang dilanggar haknya sebagaimana dimaksud pada ayat (1) dapat mengajukan gugatan atas kerugian yang ditimbulkan berdasarkan Undang-Undang ini.

(3) Setiap Penyelenggara Sistem Elektronik wajib menghapus Informasi Elektronik dan/atau Dokumen Elektronik yang tidak relevan yang berada di bawah kendalinya atas permintaan Orang yang bersangkutan berdasarkan penetapan pengadilan.

(4) Setiap Penyelenggara Sistem Elektronik wajib menyediakan mekanisme penghapusan Informasi Elektronik dan/atau Dokumen Elektronik yang sudah tidak relevan sesuai dengan ketentuan peraturan perundang-undangan.

(5) Ketentuan mengenai tata cara penghapusan Informasi Elektronik dan/ atau Dokumen Elektronik sebagaimana dimaksud pada ayat (3) dan ayat (4) diatur dalam peraturan pemerintah.

BAB VII

PERBUATAN YANG DILARANG

Pasal 27

(1) Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan.

Penjelasan Pasal 27 Ayat (1):

Yang dimaksud dengan "mendistribusikan" adalah mengirimkan dan/atau menyebarkan Informasi Elektronik dan/atau Dokumen Eletronik kepada banyak orang atau berbagai

a. *A privacy right is the right to enjoy personal life and be free from any invasion.*

b. *A privacy right is the right to communicate with other Persons without surveillance.*

c. *A privacy right is the right to inspect access to information about personal life of and data on individuals.*

(2) Any Person whose rights are infringed as referred to in section (1) may file a claim for harm incurred under this Law.

(3) Any Electronic System Provider must, at the request of the Person concerned upon a court order, delete irrelevant Electronic Information and/or Electronic Records under their control. (The right to be forgotten)

(4) Any Electronic System Provider must provide the mechanism for deletion of irrelevant Electronic Information and/or Electronic Records under the laws and regulations. (The right to be forgotten)

(5) Ancillary provisions for procedures for deletion of Electronic Information and/or Electronic Records as referred to in section (3) and section (4) shall be governed by regulation of the government. (The right to be forgotten)

CHAPTER VII

PROHIBITED ACTS

Article 27

(1) No Person shall intentionally and unauthorizedly distribute and/or transmit and/or cause to be accessible Electronic Information and/or Electronic Records with contents against propriety.

Elucidation of Article 27 Section (1):

"Distribute" means send and/or disseminate Electronic Information and/or Electronic Records to many people or various parties by means of Electronic Systems.

pihak melalui Sistem Elektronik.

Yang dimaksud dengan "mentransmisikan" adalah mengirimkan Informasi Elektronik dan/atau Dokumen Eletronik yang ditujukan kepada satu pihak lain melalui Sistem Elektronik.

Yang dimaksud dengan "membuat dapat diakses" adalah semua perbuatan lain selain mendistribusikan dan mentransmisikan melalui Sistem Elektronik yang menyebabkan Informasi Elektronik dan/atau Dokumen Elektronik dapat diketahui pihak lain atau publik.

(2) Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan perjudian.

(3) Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan penghinaan dan/atau pencemaran nama baik.

<u>Penjelasan Pasal 27 Ayat (3):</u>

Ketentuan dalam ayat ini mengacu pada ketentuan pencemaran nama baik dan/atau fitnah yang diatur dalam Kitab Undang-Undang Hukum Pidana (KUHP).

(4) Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan pemerasan dan/atau pengancaman.

<u>Penjelasan Pasal 27 Ayat (4):</u>

Ketentuan pada ayat ini mengacu pada ketentuan pemerasan dan/atau pengancaman yang diatur dalam Kitab Undang-Undang Hukum Pidana (KUHP).

Pasal 28

(1) Setiap Orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik.

(2) Setiap Orang dengan sengaja dan tanpa hak menyebarkan informasi yang ditujukan untuk

"Transmit" means send Electronic Information and/or Electronic Records to another party by means of Electronic Systems.

"Cause to be accessible" means any act other than distribute and transmit that is committed by means of Electronic Systems and causes Electronic Information and/or Electronic Records to become other parties' or public knowledge.

(2) No Person shall intentionally and unauthorizedly distribute and/or transmit and/or cause to be accessible Electronic Information and/or Electronic Records with contents of gaming.

(3) No Person shall intentionally and unauthorizedly distribute and/or transmit and/or cause to be accessible Electronic Information and/or Electronic Records with contents of affronts and/or defamation.

<u>Elucidation of Article 27 Section (3):</u>

The provision of this section shall refer to the provisions for defamation and/or slander as governed by the Criminal Code.

(4) No Person shall intentionally and unauthorizedly distribute and/or transmit and/or cause to be accessible Electronic Information and/or Electronic Records with contents of extortion and/or threats.

<u>Elucidation of Article 27 Section (4):</u>

The provision of this section shall refer to the provisions for extortion and/or threats as governed by the Criminal Code.

Article 28

(1) No Person shall intentionally and unauthorizedly disseminate false and misleading information resulting in consumer loss in Electronic Transactions.

(2) No Person shall intentionally and unauthorizedly disseminate information with

menimbulkan rasa kebencian atau permusuhan individu dan/atau kelompok masyarakat tertentu berdasarkan atas suku, agama, ras, dan antargolongan (SARA).

intent to incite hatred or dissension on individuals and/or certain groups of community on the basis of ethnic groups, religions, races, and intergroups (communal disturbances).

Pasal 29

Setiap Orang dengan sengaja dan tanpa hak mengirimkan Informasi Elektronik dan/atau Dokumen Elektronik yang berisi ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi.

Article 29

No Person shall intentionally and unauthorizedly send Electronic Information and/or Electronic Records that contain violence threats or intimidation against individuals.

Pasal 30

(1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apapun.

(2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apapun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik.

Penjelasan Pasal 30 Ayat (2):

Secara teknis perbuatan yang dilarang sebagaimana dimaksud pada ayat ini dapat dilakukan, antara lain dengan:

a. melakukan komunikasi, mengirimkan, memancarkan atau sengaja berusaha mewujudkan hal-hal tersebut kepada siapapun yang tidak berhak untuk menerimanya; atau

b. sengaja menghalangi agar informasi dimaksud tidak dapat diterima atau gagal diterima oleh yang berwenang menerimanya di lingkungan pemerintah dan/atau pemerintah daerah.

(3) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apapun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.

Penjelasan Pasal 30 Ayat (3):

Sistem pengamanan adalah sistem yang

Article 30

(1) No Person shall intentionally and unauthorizedly or unlawfully access in any manner whatsoever Computers and/or Electronic Systems belonging to other Persons.

(2) No Person shall intentionally and unauthorizedly or unlawfully access Computers and/or Electronic Systems in any manner whatsoever with intent to obtain Electronic Information and/or Electronic Records.

Elucidation of Article 30 Section (2):

Technically, such prohibited acts under this section may be committed by, inter alia:

a. communicating, sending, transmitting or intentionally attempting such information to be received by any Person who is unauthorized to receive it; or

b. intentionally inhibiting or thwarting the authorized parties within the government and/or regional governments from receiving such information.

(3) No Person shall intentionally and unauthorizedly or unlawfully access Computers and/or Electronic Systems in any manner whatsoever to breach, hack into, trespass into, or break through security systems.

Elucidation of Article 30 Section (3):

Security systems are systems that restrict access to

membatasi akses komputer atau melarang akses ke dalam komputer dengan berdasarkan kategorisasi atau klasifikasi pengguna beserta tingkatan kewenangan yang ditentukan.

computers or prohibit access to computers by category or classification of users and specified levels of the authority.

Pasal 31

Article 31

(1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atau penyadapan atas Informasi Elektronik dan/atau Dokumen Elektronik dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain.

(1) No Person shall intentionally and unauthorizedly or unlawfully carry out interception or wiretapping of Electronic Information and/or Electronic Records in certain Computers and/or Electronic Systems belonging to other Persons.

Penjelasan Pasal 31 Ayat (1):

Yang dimaksud dengan "intersepsi atau penyadapan" adalah kegiatan untuk mendengarkan, merekam, membelokkan, mengubah, menghambat, dan/atau mencatat transmisi Informasi Elektronik dan/atau Dokumen Elektronik yang tidak bersifat publik, baik menggunakan jaringan kabel komunikasi maupun jaringan nirkabel, seperti pancaran elektromagnetis atau radio frekuensi.

Elucidation of Article 31 Section (1):

"Interception or wiretapping" means activities to listen, record, reroute, alter, block, and/or log transmission of non-public Electronic Information and/or Electronic Records by means of communications wired networks or wireless networks, such as electromagnetic waves or frequency radio.

(2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atas transmisi Informasi Elektronik dan/atau Dokumen Elektronik yang tidak bersifat publik dari, ke, dan di dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain, baik yang tidak menyebabkan perubahan apapun maupun yang menyebabkan adanya perubahan, penghilangan, dan/atau penghentian Informasi Elektronik dan/atau Dokumen Elektronik yang sedang ditransmisikan.

(2) No Person shall intentionally and unauthorizedly or unlawfully carry out interception of the transmission of non-public Electronic Information and/or Electronic Records from, to, and in certain Computers and/or Electronic Systems belonging to other Persons, whether or not causing alteration, deletion, and/or blocking of Electronic Information and/or Electronic Records in transmission.

~~(3) Kecuali intersepsi sebagaimana dimaksud pada ayat (1) dan ayat (2), intersepsi yang dilakukan dalam rangka penegakan hukum atas permintaan kepolisian, kejaksaan, dan/atau institusi penegak hukum lainnya yang ditetapkan berdasarkan undang-undang.~~

~~(3) No prohibition shall be imposed against interception as referred to in section (1) and section (2) that is carried out in the scope of law enforcement at the request of the police, prosecutor's office, and/or other law enforcement institutions as provided by law.~~

(3) Ketentuan sebagaimana dimaksud pada ayat (1) dan ayat (2) tidak berlaku terhadap intersepsi atau penyadapan yang dilakukan dalam rangka penegakan hukum atas permintaan kepolisian, kejaksaan, atau institusi lainnya yang kewenangannya ditetapkan berdasarkan undang-undang.

(3) The provisions of section (1) and section (2) shall not apply to interception or wiretapping that is carried out in the scope of law enforcement at the request of the police, prosecutor's office, or other institutions whose authority to do so is provided by law.

(4) ~~Ketentuan lebih lanjut mengenai tata cara intersepsi sebagaimana dimaksud pada ayat (3) diatur dengan Peraturan Pemerintah.~~

~~**Anotasi Pasal 31 Ayat (4):**~~

~~Menurut Putusan Mahkamah Konstitusi No. 5/PUU-VIII/2010, 24 Februari 2011, Pasal 31 ayat (4) bertentangan dengan Pasal 28J ayat (2) UUD 1945 (UUD) dan tidak mempunyai kekuatan hukum mengikat.~~

~~(Pasal 28J ayat (2) UUD menetapkan bahwa dalam menjalankan hak dan kebebasannya, setiap orang wajib tunduk kepada pembatasan yang ditetapkan dengan undang-undang. Sementara itu Undang-undang Transaksi Elektronik memandatkan bahwa intersepsi/penyadapan diatur lebih lanjut oleh peraturan pemerintah. Pembatasan demikian hanya dapat diperintahkan oleh undang-undang dan undang-undang dimaksud itulah yang selanjutnya harus merumuskan, antara lain, siapa yang berwenang mengeluarkan perintah penyadapan dan perekaman pembicaraan.)~~

(4) Ketentuan lebih lanjut mengenai tata cara intersepsi sebagaimana dimaksud pada ayat (3) diatur dengan undang-undang.

Pasal 32

(1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apapun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik publik.

(2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik Orang lain yang tidak berhak.

(3) Terhadap perbuatan sebagaimana dimaksud pada ayat (1) yang mengakibatkan terbukanya suatu Informasi Elektronik dan/atau Dokumen Elektronik yang bersifat rahasia menjadi dapat diakses oleh publik dengan keutuhan data yang tidak sebagaimana mestinya.

Pasal 33

(4) ~~Ancillary provisions for procedures for interception as referred to in section (3) shall be governed by Regulation of the Government.~~

~~**Annotation of Article 31 section (4):**~~

~~Under Decision of the Constitutional Court No. 5/PUU-VIII/2010, February 24, 2011, Article 31 section (4) is against Article 28J section (2) of the 1945 Constitution and has no binding legal force and effect of law.~~

~~(Article 28J section (2) of the Constitution provides that in the exercise of his/her rights and freedom, every person must be subject to the limitation as provided by law (*undang-undang*), whereas the Electronic Transaction Law mandates that ancillary provisions for interception shall be governed by regulation of the government (*peraturan pemerintah*). Such limitation may only be mandated by law, not by regulation of the government, and that very law must further govern, inter alia, those competent to issue orders to intercept and record conversations.)~~

(4) Ancillary provisions for procedures for interception as referred to in section (3) shall be governed by law.

Article 32

(1) No Person shall intentionally and unauthorizedly or unlawfully alter, add, reduce, transmit, tamper with, delete, move, hide in any manner whatsoever Electronic Information and/or Electronic Records belonging to other Persons or the public.

(2) No Person shall intentionally and unauthorizedly or unlawfully move or transfer in any manner whatsoever Electronic Information and/or Electronic Records to Electronic Systems of unauthorized Persons.

(3) No person shall commit acts as referred to in section (1) that result in any confidential Electronic Information and/or Electronic Record being compromised such that the data, whose integrity is already compromised, become accessible to the public.

Article 33

Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan tindakan apapun yang berakibat terganggunya Sistem Elektronik dan/atau mengakibatkan Sistem Elektronik menjadi tidak bekerja sebagaimana mestinya.

No Person shall intentionally and unauthorizedly or unlawfully commits any act that results in faults on Electronic Systems and/or results in Electronic Systems working improperly.

Pasal 34

(1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum memproduksi, menjual, mengadakan untuk digunakan, mengimpor, mendistribusikan, menyediakan, atau memiliki:

    a. perangkat keras atau perangkat lunak Komputer yang dirancang atau secara khusus dikembangkan untuk memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33;

    b. sandi lewat Komputer, Kode Akses, atau hal yang sejenis dengan itu yang ditujukan agar Sistem Elektronik menjadi dapat diakses dengan tujuan memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33.

(2) Tindakan sebagaimana dimaksud pada ayat (1) bukan tindak pidana jika ditujukan untuk melakukan kegiatan penelitian, pengujian Sistem Elektronik, untuk perlindungan Sistem Elektronik itu sendiri secara sah dan tidak melawan hukum.

Penjelasan Pasal 34 Ayat (2):

Yang dimaksud dengan "kegiatan penelitian" adalah penelitian yang dilaksanakan oleh lembaga penelitian yang memiliki izin.

Article 34

(1) No Person shall intentionally and unauthorizedly or unlawfully produce, sell, procure to be used, import, distribute, provide, or own:

    a. computer hardware or software that is designed or specifically developed to facilitate acts as referred to in Article 27 through Article 33;

    b. computer passwords, Access Codes, or the like to make Electronic Systems accessible with intent to facilitate acts as referred to in Article 27 through Article 33.

(2) Acts as referred to in section (1) shall not be criminal acts if aimed at carrying out research activities, testing of Electronic Systems, protecting Electronic Systems themselves in a legal and lawful manner.

Elucidation of Article 34 Section (2):

"Research activities" means research that is conducted by licensed research institutions.

Pasal 35

Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik.

Article 35

No Person shall intentionally and unauthorizedly or unlawfully manipulate, create, alter, delete, tamper with Electronic Information and/or Electronic Records with intent that such Electronic Information and/or Electronic Records would seem to be authentic data.

Pasal 36

Setiap Orang dengan sengaja dan tanpa hak atau

Article 36

No Person shall intentionally and unauthorizedly

melawan hukum melakukan perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 34 yang mengakibatkan kerugian bagi Orang lain.

or unlawfully commit acts as referred to in Article 27 through Article 34 that cause other Persons any harm.

Pasal 37

Setiap Orang dengan sengaja melakukan perbuatan yang dilarang sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 36 di luar wilayah Indonesia terhadap Sistem Elektronik yang berada di wilayah yurisdiksi Indonesia.

Article 37

No Person shall intentionally commit prohibited acts as referred to in Article 27 through Article 36 outside the territory of Indonesia targeting Electronic Systems residing within jurisdiction of Indonesia.

BAB VIII

PENYELESAIAN SENGKETA

CHAPTER VIII

DISPUTE RESOLUTION

Pasal 38

Article 38

(1) Setiap Orang dapat mengajukan gugatan terhadap pihak yang menyelenggarakan Sistem Elektronik dan/atau menggunakan Teknologi Informasi yang menimbulkan kerugian.

(1) Any Person may bring a legal action against parties who provide Electronic Systems and/or use Information Technology in a manner causing them any harm.

(2) Masyarakat dapat mengajukan gugatan secara perwakilan terhadap pihak yang menyelenggarakan Sistem Elektronik dan/atau menggunakan Teknologi Informasi yang berakibat merugikan masyarakat, sesuai dengan ketentuan Peraturan Perundang-undangan.

(2) The public may under the laws and regulations bring a class action lawsuit against parties who provide Electronic Systems and/or use Information Technology in a manner causing the public any harm.

Pasal 39

Article 39

(1) Gugatan perdata dilakukan sesuai dengan ketentuan Peraturan Perundang-undangan.

(1) Civil actions shall be filed under the laws and regulations.

(2) Selain penyelesaian gugatan perdata sebagaimana dimaksud pada ayat (1), para pihak dapat menyelesaikan sengketa melalui arbitrase, atau lembaga penyelesaian sengketa alternatif lainnya sesuai dengan ketentuan Peraturan Perundang-undangan.

(2) In addition to resolution by civil actions as referred to in by section (1), parties may resolve disputes by arbitration or other alternative dispute resolution tribunals under the Laws and Regulations.

BAB IX

PERAN PEMERINTAH DAN PERAN MASYARAKAT

CHAPTER IX

GOVERNMENT AND PUBLIC PARTICIPATION

Pasal 40

Article 40

(1) Pemerintah memfasilitasi pemanfaatan Teknologi Informasi dan Transaksi Elektronik sesuai dengan ketentuan Peraturan Perundang-undangan.

(1) The Government shall facilitate the utilization of Information Technology and Electronic Transactions under the laws and regulations.

Penjelasan Pasal 40 Ayat (1):

Elucidation of Article 40 Section (1):

Fasilitasi pemanfaatan Teknologi Informasi, termasuk tata kelola Teknologi Informasi dan Transaksi Elektronik yang aman, beretika, cerdas, kreatif, produktif, dan inovatif. Ketentuan ini termasuk memfasilitasi masyarakat luas, instansi pemerintah, dan pelaku usaha dalam mengembangkan produk dan jasa Teknologi Informasi dan komunikasi.	***Facilitation of utilization of Information Technology includes the governance of Information Technology and Electronic Transactions which are safe, ethical, intelligent, creative, productive, and innovative. This provision includes facilitation for the general public, government agencies, and business actors in developing Information Technology and communication products and services.***
(2) Pemerintah melindungi kepentingan umum dari segala jenis gangguan sebagai akibat penyalahgunaan Informasi Elektronik dan Transaksi Elektronik yang mengganggu ketertiban umum, sesuai dengan ketentuan Peraturan Perundang-undangan.	(2) The Government shall protect the public interest from any type of threat as a result of misusing Electronic Information and Electronic Transactions that offends public order under the Laws and Regulations.
(2a) Pemerintah wajib melakukan pencegahan penyebarluasan dan penggunaan Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang dilarang sesuai dengan ketentuan peraturan perundang-undangan.	**(2a) The government must prevent any dissemination and use of Electronic Information and/or Electronic Records with contents prohibited by the laws and regulations.**
(2b) Dalam melakukan pencegahan sebagaimana dimaksud pada ayat (2a), Pemerintah berwenang melakukan pemutusan akses dan/atau memerintahkan kepada Penyelenggara Sistem Elektronik untuk melakukan pemutusan akses terhadap Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar hukum.	**(2b) To so prevent as referred to in section (2a), the government shall have the power to block access to and/or order Electronic System Providers to block access to Electronic Information and/or Electronic Records with unlawful contents.**
(3) Pemerintah menetapkan instansi atau institusi yang memiliki data elektronik strategis yang wajib dilindungi.	(3) The Government shall determine agencies or institutions holding strategic electronic data that must be protected.
(4) Instansi atau institusi sebagaimana dimaksud pada ayat (3) harus membuat Dokumen Elektronik dan rekam cadang elektroniknya serta menghubungkannya ke pusat data tertentu untuk kepentingan pengamanan data.	(4) Agencies or institutions as referred to in section (3) must create Electronic Records and the electronic backups thereof, and connect them with specified data centers in the interest of data security.
(5) Instansi atau institusi lain selain diatur pada ayat (3) membuat Dokumen Elektronik dan rekam cadang elektroniknya sesuai dengan keperluan perlindungan data yang dimilikinya.	(5) Other agencies or institutions other than those provided by section (3) shall create Electronic Records and their electronic backups as necessary to protect data they hold.
(6) Ketentuan lebih lanjut mengenai peran Pemerintah sebagaimana dimaksud pada ayat (1), ayat (2), ayat (2a), ayat (2b) dan ayat (3) diatur dalam peraturan pemerintah.	(6) Ancillary provisions for the Government participation as referred to in section (1), section (2), section (2a), section (2b) and section (3) shall be governed by regulation of

Pasal 41

(1) Masyarakat dapat berperan meningkatkan pemanfaatan Teknologi Informasi melalui penggunaan dan Penyelenggaraan Sistem Elektronik dan Transaksi Elektronik sesuai dengan ketentuan Undang-Undang ini

(2) Peran masyarakat sebagaimana dimaksud pada ayat (1) dapat diselenggarakan melalui lembaga yang dibentuk oleh masyarakat.

Penjelasan Pasal 41 Ayat (2):

Yang dimaksud dengan "lembaga yang dibentuk oleh masyarakat" merupakan lembaga yang bergerak di bidang teknologi informasi dan transaksi elektronik.

(3) Lembaga sebagaimana dimaksud pada ayat (2) dapat memiliki fungsi konsultasi dan mediasi.

BAB X

PENYIDIKAN

Pasal 42

Penyidikan terhadap tindak pidana sebagaimana dimaksud dalam Undang-Undang ini, dilakukan berdasarkan ketentuan dalam Hukum Acara Pidana dan ketentuan dalam Undang-Undang ini.

Pasal 43

(1) Selain Penyidik Pejabat Polisi Negara Republik Indonesia, Pejabat Pegawai Negeri Sipil tertentu di lingkungan Pemerintah yang lingkup tugas dan tanggung jawabnya di bidang Teknologi Informasi dan Transaksi Elektronik diberi wewenang khusus sebagai penyidik sebagaimana dimaksud dalam Undang-Undang tentang Hukum Acara Pidana untuk melakukan penyidikan tindak pidana di bidang Teknologi Informasi dan Transaksi Elektronik.

Penjelasan Pasal 43 Ayat (1):

Yang dimaksud dengan "Pejabat Pegawai Negeri Sipil tertentu" adalah Pejabat Pegawai Negeri Sipil kementerian yang menyelenggarakan urusan pemerintahan di bidang komunikasi dan informatika yang telah memenuhi persyaratan berdasarkan ketentuan

the government.

Article 41

(1) The public may participate in the improvement of the utilization of Information Technology by means and provision of Electronic Systems and Electronic Transactions under this Law.

(2) The public as referred to in section (1) may participate in institutions that the public forms.

Elucidation of Article 41 Section (2):

"Institutions that the public forms" shall be institutions that are engaged in the field of information technology and electronic transactions.

(3) Institutions as referred to in section (2) may act as consultation and mediation providers.

CHAPTER X

INVESTIGATION

Article 42

Criminal acts as referred to in this Law shall be investigated under the provisions of the Law of Criminal Procedure and the provisions of this Law.

Article 43

(1) In addition to Investigators of the State Police of the Republic of Indonesia, certain Civil Service Officials within the Government whose scope of duties and responsibilities is in the field of Information Technology and Electronic Transactions shall be granted special authority as investigators as referred to in the Law of Criminal Procedure to make investigation of criminal acts of Information Technology and Electronic Transactions.

Elucidation of Article 43 Section (1):

"Certain Civil Service Officials" means Civil Service Officials of the ministry that administers the governmental affairs in the field of communications and informatics, who are eligible under the laws and regulations.

peraturan perundang-undangan.

~~(2) 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.~~

(2) Penyidikan di bidang Teknologi Informasi dan Transaksi Elektronik sebagaimana dimaksud pada ayat (1) dilakukan dengan memperhatikan perlindungan terhadap privasi, kerahasiaan, kelancaran layanan publik, dan integritas atau keutuhan data sesuai dengan ketentuan peraturan perundang-undangan.

~~(3) Penggeledahan dan/atau penyitaan terhadap sistem elektronik yang terkait dengan dugaan tindak pidana harus dilakukan atas izin ketua pengadilan negeri setempat.~~

(3) Penggeledahan dan/atau penyitaan terhadap Sistem Elektronik yang terkait dengan dugaan tindak pidana di bidang Teknologi Informasi dan Transaksi Elektronik dilakukan sesuai dengan ketentuan hukum acara pidana.

(4) Dalam melakukan penggeledahan dan/atau penyitaan sebagaimana dimaksud pada ayat (3), penyidik wajib menjaga terpeliharanya kepentingan pelayanan umum.

~~(5) Penyidik Pegawai Negeri Sipil sebagaimana dimaksud pada ayat (1) berwenang:~~

~~a. menerima laporan atau pengaduan dari seseorang tentang adanya tindak pidana berdasarkan ketentuan Undang-Undang ini;~~

~~b. memanggil setiap Orang atau pihak lainnya untuk didengar dan/atau diperiksa sebagai tersangka atau saksi sehubungan dengan adanya dugaan tindak pidana di bidang terkait dengan ketentuan Undang-Undang ini;~~

~~(2) Investigation of Information Technology and Electronic Transactions as referred to in section (1) shall be made with due regard to the protection of privacy, secrecy, seamless public services, data integrity, or validity of data under the laws and regulations.~~

(2) Investigation of Information Technology and Electronic Transactions as referred to in section (1) shall be made with due regard to the protection of privacy, secrecy, seamless public services, and data integrity or validity under the laws and regulations.

~~(3) Searches and/or seizures of electronic systems that are suspected of being complicit in criminal acts must be carried out with the permission of the local chief judge of the district court.~~

(3) Searches and/or seizures of Electronic Systems that are suspected of being complicit in criminal acts in the field of Information Technology and Electronic Transactions shall be carried out under the provisions of the law of criminal procedure.

(4) In carrying out searches and/or seizures as referred to in section (3), investigators must maintain the public service interests.

~~(5) Civil Service Investigators as referred to in section (1) shall be authorized to:~~

~~a. receive reports or complaints from a person of the occurrence of criminal acts under this Law;~~

~~b. summons any Person or other party for hearing and/or examination as a suspect or witness in connection with the suspected criminal acts in the field related to the provisions of this Law;~~

c. melakukan pemeriksaan atas kebenaran laporan atau keterangan berkenaan dengan tindak pidana berdasarkan ketentuan Undang-Undang ini;

d. melakukan pemeriksaan terhadap Orang dan/atau Badan Usaha yang patut diduga melakukan tindak pidana berdasarkan Undang-Undang ini;

e. melakukan pemeriksaan terhadap alat dan/atau sarana yang berkaitan dengan kegiatan Teknologi Informasi yang diduga digunakan untuk melakukan tindak pidana berdasarkan Undang-Undang ini;

f. melakukan penggeledahan terhadap tempat tertentu yang diduga digunakan sebagai tempat untuk melakukan tindak pidana berdasarkan ketentuan Undang-Undang ini;

g. melakukan penyegelan dan penyitaan terhadap alat dan/atau sarana kegiatan Teknologi Informasi yang diduga digunakan secara menyimpang dari ketentuan peraturan perundang-undangan;

h. meminta bantuan ahli yang diperlukan dalam penyidikan terhadap tindak pidana berdasarkan Undang-Undang ini; dan/atau

Penjelasan Pasal 43 Ayat (5) Huruf h:

Yang dimaksud "ahli" adalah seseorang yang memiliki keahlian khusus di bidang Teknologi Informasi yang dapat dipertanggungjawabkan secara akademis maupun praktis mengenai pengetahuannya tersebut.

i. mengadakan penghentian penyidikan tindak pidana berdasarkan Undang-Undang ini sesuai dengan ketentuan hukum acara pidana yang berlaku.

(5) Penyidik Pegawai Negeri Sipil sebagaimana dimaksud pada ayat (1) berwenang:

a. menerima laporan atau pengaduan dari seseorang tentang adanya tindak pidana di bidang Teknologi Informasi

c. verify reports or inquiries into criminal acts under the provisions of this Law;

d. examine Persons and/or Business Entities that should be suspected of having committed criminal acts under this Law;

e. inspect equipment and/or facilities in connection with the activities of Information Technology that is suspected of having been used to commit criminal acts under this Law;

f. search certain places that are suspected of having been used as the place to commit criminal acts under the provisions of this Law;

g. seal and seize equipment and/or facilities of Information Technology activities suspected of having been used in a manner non-compliant with the Laws and Regulations;

h. seek assistance from experts as necessary for investigation of criminal acts under this Law; and/or

Elucidation of Article 43 Section (5) Point h:

"Expert" means a Person who has special expertise in the field of Information Technology, and whose knowledge thereof is academically or practically reliable.

i. cease investigation of criminal acts under this Law in accordance with the provisions of the prevailing law of criminal procedure.

(5) Civil Service Investigators as referred to in section (1) shall be authorized to:

a. receive reports or complaints from a person of the occurrence of criminal acts in the field of Information

dan Transaksi Elektronik;

b. memanggil setiap Orang atau pihak lainnya untuk didengar dan diperiksa sebagai tersangka atau saksi sehubungan dengan adanya dugaan tindak pidana di bidang Teknologi Informasi dan Transaksi Elektronik;

c. melakukan pemeriksaan atas kebenaran laporan atau keterangan berkenaan dengan tindak pidana di bidang Teknologi Informasi dan Transaksi Elektronik;

d. melakukan pemeriksaan terhadap Orang dan/atau Badan Usaha yang patut diduga melakukan tindak pidana di bidang Teknologi Informasi dan Transaksi Elektronik;

e. melakukan pemeriksaan terhadap alat dan/atau sarana yang berkaitan dengan kegiatan Teknologi Informasi yang diduga digunakan untuk melakukan tindak pidana di bidang Teknologi Informasi dan Transaksi Elektronik;

f. melakukan penggeledahan terhadap tempat tertentu yang diduga digunakan sebagai tempat untuk melakukan tindak pidana di bidang Teknologi Informasi dan Transaksi Elektronik;

g. melakukan penyegelan dan penyitaan terhadap alat dan/atau sarana kegiatan Teknologi Informasi yang diduga digunakan secara menyimpang dari ketentuan peraturan perundang-undangan;

h. membuat suatu data dan/atau Sistem Elektronik yang terkait tindak pidana di bidang Teknologi Informasi dan Transaksi Elektronik agar tidak dapat diakses;

i. meminta informasi yang terdapat di dalam Sistem Elektronik atau informasi yang dihasilkan oleh Sistem Elektronik kepada Penyelenggara

Technology and Electronic Transactions;

b. summons any Person or other party for hearing and examination as a suspect or witness in connection with the suspected criminal acts in the field of Information Technology and Electronic Transactions;

c. verify reports or inquiries into criminal acts in the field of Information Technology and Electronic Transactions;

d. examine Persons and/or Business Entities that should be suspected of having committed criminal acts in the field of Information Technology and Electronic Transactions;

e. inspect equipment and/or facilities in connection with the activities of Information Technology that is suspected of having been used to commit criminal acts in the field of Information Technology and Electronic Transactions;

f. search certain places that are suspected of having been used as the place to commit criminal acts in the field of Information Technology and Electronic Transactions;

g. seal and seize equipment and/or facilities of Information Technology activities that are suspected of having been used in a manner not compliant with the laws and regulations;

h. cause data and/or Electronic Systems that are complicit in criminal acts in the field of Information Technology and Electronic Transactions inaccessible;

i. request information in the Electronic Systems or information generated by Electronic Systems from Electronic System Providers that are complicit in

Sistem Elektronik yang terkait dengan tindak pidana di bidang Teknologi Informasi dan Transaksi Elektronik;

j. meminta bantuan ahli yang diperlukan dalam penyidikan terhadap tindak pidana di bidang Teknologi Informasi dan Transaksi Elektronik; dan/atau

k. mengadakan penghentian penyidikan tindak pidana di bidang Teknologi Informasi dan Transaksi Elektronik sesuai dengan ketentuan hukum acara pidana.

~~(6) Dalam hal melakukan penangkapan dan penahanan, penyidik melalui penuntut umum wajib meminta penetapan ketua pengadilan negeri setempat dalam waktu satu kali dua puluh empat jam.~~

(6) Penangkapan dan penahanan terhadap pelaku tindak pidana di bidang Teknologi Informasi dan Transaksi Elektronik dilakukan sesuai dengan ketentuan hukum acara pidana.

~~(7) Penyidik Pegawai Negeri Sipil sebagaimana dimaksud pada ayat (1) berkoordinasi dengan Penyidik Pejabat Polisi Negara Republik Indonesia memberitahukan dimulainya penyidikan dan menyampaikan hasilnya kepada penuntut umum.~~

(7) Penyidik Pejabat Pegawai Negeri Sipil sebagaimana dimaksud pada ayat (1) dalam melaksanakan tugasnya memberitahukan dimulainya penyidikan kepada Penuntut Umum melalui Penyidik Pejabat Polisi Negara Republik Indonesia.

(7a) Dalam hal penyidikan sudah selesai, Penyidik Pejabat Pegawai Negeri Sipil sebagaimana dimaksud pada ayat (1) menyampaikan hasil penyidikannya kepada Penuntut Umum melalui Penyidik Pejabat Polisi Negara Republik Indonesia.

~~(8) Dalam rangka mengungkap tindak pidana Informasi Elektronik dan Transaksi Elektronik, penyidik dapat bekerja sama dengan penyidik negara lain untuk berbagi informasi dan alat bukti.~~

criminal acts in the field of Information Technology and Electronic Transactions;

j. seek assistance from experts as necessary for investigation of criminal acts in the field of Information Technology and Electronic Transactions; and/or

k. cease investigation of criminal acts in the field of Information Technology and Electronic Transactions under the provisions of the law of criminal procedure.

~~(6) To make arrest and detention, investigators through public prosecutors must seek order of the local chief judge of the district court within one period of twenty-four hours.~~

(6) Arrest and detention of perpetrators of Information Technology and Electronic Transactions shall be made under the provisions of the law of criminal procedure.

~~(7) Civil Service Investigators as referred to in section (1) shall coordinate with Investigators of the State Police of the Republic of Indonesia to notify the commencement of investigation and deliver the findings thereof to the public prosecutors.~~

(7) Civil Service Investigators as referred to in section (1) shall, in the performance of their duties, notify the initiation of investigation to the Public Prosecutors through the Investigators of the State Police of the Republic of Indonesia.

(7a) Upon completion of the investigation, Civil Service Investigators as referred to in section (1) shall submit the investigation findings to the Public Prosecutors through the Investigators of the State Police of the Republic of Indonesia.

~~(8) To uncover criminal acts of Electronic Information and Electronic Transactions, investigators may cooperate with investigators of other countries to share information and means of proof.~~

(8) Dalam rangka mengungkap tindak pidana Informasi Elektronik dan Transaksi Elektronik, penyidik dapat bekerja sama dengan penyidik negara lain untuk berbagi informasi dan alat bukti sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 44

Alat bukti penyidikan, penuntutan dan pemeriksaan di sidang pengadilan menurut ketentuan Undang-Undang ini adalah sebagai berikut:

a. alat bukti sebagaimana dimaksud dalam ketentuan Perundang-undangan; dan

b. alat bukti lain berupa Informasi Elektronik dan/atau Dokumen Elektronik sebagaimana dimaksud dalam Pasal 1 angka 1 dan angka 4 serta Pasal 5 ayat (1), ayat (2), dan ayat (3).

Anotasi Pasal 44 huruf b:

Menurut Putusan Mahkamah Konstitusi No. 20/PUU-XIV/2016, 7 September 2016, frasa "Informasi Elektronik dan/atau Dokumen Elektronik" bertentangan dengan UUD 1945 dan tidak mempunyai kekuatan hukum mengikat sepanjang tidak dimaknai khususnya frasa "Informasi Elektronik dan/atau Dokumen Elektronik" sebagai alat bukti dilakukan dalam rangka penegakan hukum atas permintaan kepolisian, kejaksaan, dan/atau institusi penegak hukum lainnya yang ditetapkan berdasarkan undang-undang sebagaimana ditentukan dalam Pasal 31 ayat (3).

BAB XI

KETENTUAN PIDANA

Pasal 45

~~(1) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 27 ayat (1), ayat (2), ayat (3), atau ayat (4) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).~~

~~(2) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 28 ayat (1) atau ayat (2) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00~~

(8) To uncover criminal acts of Electronic Information and Electronic Transactions, Civil Service Investigators may cooperate with investigators of other countries to share information and means of proof under the laws and regulations.

Article 44

Means of proof on the investigation, prosecution and examination at court under the provisions of this Law shall be as follows:

a. means of proof as referred to in the laws and regulations; and

b. other means of proof in the form of Electronic Information and/or Electronic Records as referred to in Article 1 point 1 and point 4 as well as Article 5 section (1), section (2), and section (3).

Annotation of Article 44 point (b):

Under Decision of the Constitutional Court No. 20/PUU-XIV/2016, September 7, 2016, the phrases "Electronic Information and/or Electronic Records" are against the 1945 Constitutional Law and have no binding force and effect of law, as long as the phrases, especially "Electronic Information and/or Electronic Records," are not meant to act as means of proof that is made in the scope of law enforcement at the request of the police, prosecutor's office, and/or other law enforcement institutions as provided by law under Article 31 section (3).

CHAPTER XI

PENAL PROVISIONS

Article 45

~~(1) Any Person who satisfies the elements of Article 27 section (1), section (2), section (3), or section (4) shall be sentenced to imprisonment of at most 6 (six) years and/or a fine of at most Rp1,000,000,000 (one billion rupiah).~~

~~(2) Any Person who satisfies the elements of Article 28 section (1) or section (2) shall be sentenced to imprisonment of at most 6 (six) years and/or a fine of at most Rp1,000,000,000 (one billion rupiah).~~

~~(satu miliar rupiah).~~

~~(3) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 29 dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp2.000.000.000,00 (dua miliar rupiah).~~

~~(3) Any Person who satisfies the elements of Article 29 shall be sentenced to imprisonment of at most 12 (twelve) years and/or a fine of at most Rp2,000,000,000 (two billion rupiah).~~

(1) Setiap Orang yang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan sebagaimana dimaksud dalam Pasal 27 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).

(1) Any Person who intentionally and unauthorizedly distributes and/or transmits and/or causes to be accessible Electronic Information and/or Electronic Records with contents against propriety as referred to in Article 27 section (1) shall be sentenced to imprisonment of at most 6 (six) years and/or a fine of at most Rp1,000,000,000 (one billion rupiah).

(2) Setiap Orang yang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan perjudian sebagaimana dimaksud dalam Pasal 27 ayat (2) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).

(2) Any Person who intentionally and unauthorizedly distributes and/or transmits and/or causes to be accessible Electronic Information and/or Electronic Records with contents against gaming as referred to in Article 27 section (2) shall be sentenced to imprisonment of at most 6 (six) years and/or a fine of at most Rp1,000,000,000 (one billion rupiah).

(3) Setiap Orang yang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan penghinaan atau pencemaran nama baik sebagaimana dimaksud dalam Pasal 27 ayat (3) dipidana dengan pidana penjara paling lama 4 (empat) tahun dan/atau denda paling banyak Rp750.000.000,00 (tujuh ratus lima puluh juta rupiah).

(3) Any Person who intentionally and unauthorizedly distributes and/or transmits and/or causes to be accessible Electronic Information and/or Electronic Records with contents of affronts or defamation as referred to in Article 27 section (3) shall be sentenced to imprisonment of at most 4 (four) years and/or a fine of at most Rp750,000,000 (seven hundred fifty million rupiah).

(4) Setiap Orang yang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan pemerasan dan/atau pengancaman sebagaimana dimaksud dalam Pasal 27 ayat (4) dipidana dengan pidana penjara

(4) Any Person who intentionally and unauthorizedly distributes, transmits, and/or causes to be accessible Electronic Information and/or Electronic Records with contents of extortion and/or threats as referred to in Article 27 section (4) shall be sentenced to imprisonment of at most 6 (six) years and/or a fine of at most

paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).

(5) Ketentuan sebagaimana dimaksud pada ayat (3) merupakan delik aduan.

Pasal 45A

(1) Setiap Orang yang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik sebagaimana dimaksud dalam Pasal 28 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).

(2) Setiap Orang yang dengan sengaja dan tanpa hak menyebarkan informasi yang ditujukan untuk menimbulkan rasa kebencian atau permusuhan individu dan/atau kelompok masyarakat tertentu berdasarkan atas suku, agama, ras, dan antargolongan (SARA) sebagaimana dimaksud dalam Pasal 28 ayat (2) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).

Pasal 45B

Setiap Orang yang dengan sengaja dan tanpa hak mengirimkan Informasi Elektronik dan/atau Dokumen Elektronik yang berisi ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi sebagaimana dimaksud dalam Pasal 29 dipidana dengan pidana penjara paling lama 4 (empat) tahun dan/atau denda paling banyak Rp750.000.000,00 (tujuh ratus lima puluh juta rupiah).

Penjelasan Pasal 45B:

Ketentuan dalam Pasal ini termasuk juga di dalamnya perundungan di dunia siber (*cyber bullying*) yang mengandung unsur ancaman kekerasan atau menakut-nakuti dan mengakibatkan kekerasan fisik, psikis, dan/atau kerugian materiil.

Rp1,000,000,000 (one billion rupiah).

(5) The provision of section (3) shall be a criminal complaint.

Article 45A

(1) Any Person who intentionally and unauthorizedly disseminates false and misleading information resulting in consumer loss in Electronic Transactions as referred to in Article 28 section (1) shall be sentenced to imprisonment of at most 6 (six) years and/or a fine of at most Rp1,000,000,000 (one billion rupiah).

(2) Any Person who intentionally and unauthorizedly disseminates information with intent to incite hatred or dissension on individuals and/or certain groups of community on the basis of ethnic groups, religions, races, and intergroups (communal disturbances) as referred to in Article 28 section (2) shall be sentenced to imprisonment of at most 6 (six) years and/or a fine of at most Rp1,000,000,000 (one billion rupiah).

Article 45B

Any Person who intentionally and unauthorizedly sends Electronic Information and/or Electronic Records that contain violence threats or intimidation against individuals as referred to in Article 29 shall be sentenced to imprisonment of at most 4 (four) years and/or a fine of at most Rp750,000,000 (seven hundred fifty million rupiah).

Elucidation of Article 45B:

The provision of this Article includes cyber bullying that poses the elements of violence threats or intimidation, and results in physical violence, psychic disturbances, and/or material loss.

Pasal 46

(1) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp600.000.000,00 (enam ratus juta rupiah).

(2) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (2) dipidana dengan pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp700.000.000,00 (tujuh ratus juta rupiah).

(3) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (3) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp800.000.000,00 (delapan ratus juta rupiah).

Pasal 47

Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 31 ayat (1) atau ayat (2) dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp800.000.000,00 (delapan ratus juta rupiah).

Pasal 48

(1) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (1) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp2.000.000.000,00 (dua miliar rupiah).

(2) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (2) dipidana dengan pidana penjara paling lama 9 (sembilan) tahun dan/atau denda paling banyak Rp3.000.000.000,00 (tiga miliar rupiah).

(3) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (3) dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah).

Article 46

(1) Any Person who satisfies the elements of Article 30 section (1) shall be sentenced to imprisonment of at most 6 (six) years and/or a fine of at most Rp600,000,000 (six hundred million rupiah).

(2) Any Person who satisfies the elements of Article 30 section (2) shall be sentenced to imprisonment of at most 7 (seven) years and/or a fine of at most Rp700,000,000 (seven hundred million rupiah).

(3) Any Person who satisfies the elements of Article 30 section (3) shall be sentenced to imprisonment of at most 8 (eight) years and/or a fine of at most Rp800,000,000 (eight hundred million rupiah).

Article 47

Any Person who satisfies the elements of Article 31 section (1) or section (2) shall be sentenced to imprisonment of at most 10 (ten) years and/or a fine of at most Rp800,000,000 (eight hundred million rupiah).

Article 48

(1) Any Person who satisfies the elements of Article 32 section (1) shall be sentenced to imprisonment of at most 8 (eight) years and/or a fine of at most Rp2,000,000,000 (two billion rupiah).

(2) Any Person who satisfies the elements of Article 32 section (2) shall be sentenced to imprisonment of at most 9 (nine) years and/or a fine of at most Rp3,000,000,000 (three billion rupiah).

(3) Any Person who satisfies the elements of Article 32 section (3) shall be sentenced to imprisonment of at most 10 (ten) years and/or a fine of at most Rp5,000,000,000 (five billion rupiah).

Pasal 49

Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 33, dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp10.000.000.000,00 (sepuluh miliar rupiah).

Article 49

Any Person who satisfies the elements of Article 33 shall be sentenced to imprisonment of at most 10 (ten) years and/or a fine of at most Rp10,000,000,000 (ten billion rupiah).

Pasal 50

Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 34 ayat (1) dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp10.000.000.000,00 (sepuluh miliar rupiah).

Article 50

Any Person who satisfies the elements of Article 34 section (1) shall be sentenced to imprisonment of at most 10 (ten) years and/or a fine of at most Rp10,000,000,000 (ten billion rupiah).

Pasal 51

(1) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 35 dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp12.000.000.000,00 (dua belas miliar rupiah).

(2) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 36 dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp12.000.000.000,00 (dua belas miliar rupiah).

Article 51

(1) Any Person who satisfies the elements of Article 35 shall be sentenced to imprisonment of at most 12 (twelve) years and/or a fine of at most Rp12,000,000,000 (twelve billion rupiah).

(2) Any Person who satisfies the elements as referred to in Article 36 shall be sentenced to imprisonment of at most 12 (twelve) years and/or a fine of at most Rp12,000,000,000 (twelve billion rupiah).

Pasal 52

(1) Dalam hal tindak pidana sebagaimana dimaksud dalam Pasal 27 ayat (1) menyangkut kesusilaan atau eksploitasi seksual terhadap anak dikenakan pemberatan sepertiga dari pidana pokok.

(2) Dalam hal perbuatan sebagaimana dimaksud dalam Pasal 30 sampai dengan Pasal 37 ditujukan terhadap Komputer dan/atau Sistem Elektronik serta Informasi Elektronik dan/atau Dokumen Elektronik milik Pemerintah dan/atau yang digunakan untuk layanan publik dipidana dengan pidana pokok ditambah sepertiga.

(3) Dalam hal perbuatan sebagaimana dimaksud dalam Pasal 30 sampai dengan Pasal 37 ditujukan terhadap Komputer dan/atau Sistem Elektronik serta Informasi Elektronik dan/atau Dokumen Elektronik milik Pemerintah

Article 52

(1) Criminal acts as referred to in Article 27 section (1) involving propriety or sexual exploitation of children shall be subject to an increase in the sentence by one-third of the basic sentence.

(2) Criminal acts as referred to in Article 30 through Article 37 targeting Computers and/or Electronic Systems as well as Electronic Information and/or Electronic Records belonging to the Government and/or used for public services shall be sentenced to the basic sentence plus one-third.

(3) Criminal acts as referred to in Article 30 through Article 37 targeting Computers and/or Electronic Systems as well as Electronic Information and/or Electronic Records belonging to the Government and/or

dan/atau badan strategis termasuk dan tidak terbatas pada lembaga pertahanan, bank sentral, perbankan, keuangan, lembaga internasional, otoritas penerbangan diancam dengan pidana maksimal ancaman pidana pokok masing-masing Pasal ditambah dua pertiga.

(4) Dalam hal tindak pidana sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 37 dilakukan oleh korporasi dipidana dengan pidana pokok ditambah dua pertiga.

Penjelasan Pasal 52 Ayat (4):

Ketentuan ini dimaksudkan untuk menghukum setiap perbuatan melawan hukum yang memenuhi unsur sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 37 yang dilakukan oleh korporasi (corporate crime) dan/atau oleh pengurus dan/atau staf yang memiliki kapasitas untuk:

a. mewakili korporasi;

b. mengambil keputusan dalam korporasi;

c. melakukan pengawasan dan pengendalian dalam korporasi;

d. melakukan kegiatan demi keuntungan korporasi.

BAB XII

KETENTUAN PERALIHAN

Pasal 53

Pada saat berlakunya Undang-Undang ini, semua Peraturan Perundang-undangan dan kelembagaan yang berhubungan dengan pemanfaatan Teknologi Informasi yang tidak bertentangan dengan Undang-Undang ini dinyatakan tetap berlaku.

BAB XIII

KETENTUAN PENUTUP

Pasal 54

(1) Undang-undang ini mulai berlaku pada tanggal diundangkan.

(2) Peraturan Pemerintah harus sudah ditetapkan paling lama 2 (dua) tahun setelah diundangkannya Undang-Undang ini.

Agar setiap orang mengetahuinya, memerintahkan pengundangan Undang-Undang ini dengan

the strategic agencies including but not limited to defense institutions, the central bank, banking, finance, international institutions, aviation authority shall be subject to a maximum sentence of the basic sentence for the respective Articles with an increase in the sentence by two-thirds.

(4) Criminal acts as referred to in Article 27 through Article 37 committed by corporations shall be sentenced to the basic sentence with an increase in the sentence by two-thirds.

Elucidation of Article 52 Section (4):

This provision is intended to sentence any unlawful act that satisfies the elements of Article 27 through Article 37 committed by corporations (corporate crimes) and/or by the management and/or staff with capacity to:

a. represent the corporations;

b. make decisions for the corporations;

c. make supervision and control over the corporations;

d. carry out activities for the benefit of the corporations.

CHAPTER XII

TRANSITIONAL PROVISIONS

Article 53

Upon this Law coming into effect, all Laws and Regulations and institutions in connection with utilization of Information Technology that are not against this Law are declared to remain valid.

CHAPTER XIII

CONCLUDING PROVISIONS

Article 54

(1) This law shall come into effect from the date it is promulgated.

(2) Regulation of the Governments must have been enacted not longer than 2 (two) years upon promulgation of this Law.

In order that every person may know of it, the promulgation of this Law is ordered by placement

penempatannya dalam Lembaran Negara Republik Indonesia.

Disahkan di Jakarta
pada tanggal 21 April 2008
PRESIDEN REPUBLIK INDONESIA
ttd.

DR. H. SUSILO BAMBANG YUDHOYONO

Diundangkan di Jakarta
pada tanggal 21 April 2008
MENTERI HUKUM DAN HAK ASASI MANUSIA REPUBLIK INDONESIA,
ttd
ANDI MATTALATTA

LEMBARAN NEGARA REPUBLIK INDONESIA TAHUN 2008 NOMOR 58

TAMBAHAN LEMBARAN NEGARA REPUBLIK INDONESIA NOMOR 4843

in the State Gazette of the Republic of Indonesia.

Ratified in Jakarta
on April 21, 2008
PRESIDENT OF THE REPUBLIC OF INDONESIA
sgd.
DR. H. SUSILO BAMBANG YUDHOYONO

Promulgated in Jakarta
on April 21, 2008
MINISTER OF LAW AND HUMAN RIGHTS OF THE REPUBLIC OF INDONESIA,
sgd.
ANDI MATTALATTA

STATE GAZETTE OF THE REPUBLIC OF INDONESIA NUMBER 58 OF 2008

SUPPLEMENT TO THE STATE GAZETTE OF THE REPUBLIC OF INDONESIA NUMBER 4843

***

Translated by Wishnu Basuki
wbasuki@gmail.com