PERLINDUNGAN HUKUM DATA PRIVASI MELALUI PENGGUNAAN TEKNOLOGI ENKRIPSI

Skripsi

Oleh

THANIA CHRISTY CORNE

FAKULTAS HUKUM
UNIVERSITAS LAMPUNG
BANDAR LAMPUNG
2019

ABSTRAK

Perlindungan Hukum Data Privasi melalui Penggunaan Teknologi Enkripsi

THANIA CHRISTY CORNE

Enkripsi, sistem pengkodean untuk mengacak data dengan menggunakan algoritma, berfungsi untuk menyembunyikan data privasi dari pihak ketiga. Pada mulanya, enkripsi dipakai sebagai pelindung data privasi, akan tetapi pada perkembangannya enkripsi melahirkan permasalahan di bidang hukum. Pelaku kejahatan menggunakan enkripsi sebagai perisai. Oleh karena itu, muncul permasalahan hukum apakah dengan alasan keamanan pemerintah atau negara dapat memiliki akses membuka (dekripsi) data privasi. Bagaimakah hukum internasional dan hukum Indonesia mengatur persoalan penggunaan dekripsi terhadap teknologi enkripsi.

Penulisan skripsi ini menggunakan metode yuridis normatif. Sumber data yang dipakai diambil dari data sekunder, bahan hukum primer, bahan hukum sekunder, dan bahan hukum tersier, sedangkan pengumpulan data menggunakan metode studi pustaka. Data dianalisis dengan metode analisis kualitatif.

Hasil penelitian menunjukkan bahwa pengaturan mengenai penggunaan teknologi enkripsi dalam level internasional ada dalam *guidelines* seperti *The OECD Guidelines for The Protection of Privacy and Transborder Flows of Private Data* dan *Amnesty International Policy on Encryption*, namun *guidelines* tersebut belum diterapkan secara global. *The OECD Guidelines for The Protection of Privacy and Transborder Flows of Private Data* dan *Amnesty International Policy on Encryption* memperbolehkan negara untuk mendekripsi data privasi individu atas dasar kedaulatan, keamanan nasional dan kebijakan publik. Penelitian ini juga menemukan peraturan dalam *UN Guiding Principle on Business and Human Rights* yang menegaskan bahwa perusahaan (perusahaan penyedia jasa dan layanan enkripsi) memiliki tanggung jawab untuk menghormati hak asasi manusia secara independen dan terlepas dari kemampuan dan kemauan negara. Dalam hukum Indonesia belum ada pengaturan secara khusus mengenai enkripsi. Aturan mengenai penggunaan enkripsi tersebar dalam berbagai peraturan perundang-undangan. Pengaturan dalam sistem hukum Indonesia pun menyatakan bahwa tindakan dekripsi pemerintah dinyatakan legal dengan dalih sebagai upaya penegakan hukum.

Kata Kunci: enkripsi, data privasi, keamanan nasional.

ABSTRACT

Legal Protection of Privacy Data through The Use of Encryption Technology

THANIA CHRISTY CORNE

Encryption, a coding system for scrambling data using an algorithm, serves to hide privacy data from third parties. Initially, encryption was used as a privacy data protector, but in its development encryption gave birth to problems in the legal field. Perpetrators use encryption as a shield. Therefore, legal issues arise whether for reasons of government or state security can have access to open (decrypt) privacy data. How does international law and Indonesian law regulate the issue of using decryption of encryption technology.

The writing of this thesis uses a normative juridical method. Sources of data used are taken from secondary data, primary legal materials, secondary legal materials, and tertiary legal materials, while data collection uses literature study methods. Data were analyzed by qualitative analysis methods.

The results of the study indicate that the regulation regarding the use of encryption technology in international level is in guidelines such as the OECD Guidelines for the Protection of Privacy and Transborder Flows of Private Data and Amnesty International Policy on Encryption, but these guidelines have not been applied globally. The OECD Guidelines for the Protection of Privacy and Transborder Flows of Private Data and Amnesty International Policy on Encryption allow states to decrypt private data on the basis of sovereignty, national security and public policy. This study also found that in the UN the Guiding Principle on Business and Human Rights affirms that companies have a responsibility to respect human rights independently and regardless of the ability and willingness of the state. In Indonesian law there is no specific regulation regarding encryption. Rules regarding the use of encryption are spread in various laws and regulations. The Indonesian regulation also stated that the decryption action of the government was declared legal with the pretext of being a law enforcement effort.

Keywords: encryption, data privacy, national security.

PERLINDUNGAN HUKUM DATA PRIVASI MELALUI PENGGUNAAN TEKNOLOGI ENKRIPSI

Oleh

THANIA CHRISTY CORNE

Skripsi

Sebagai salah satu syarat untuk mencapai gelar
SARJANA HUKUM

Pada

Bagian Hukum Internasional
Fakultas Hukum Universitas Lampung

FAKULTAS HUKUM
UNIVERSITAS LAMPUNG
BANDAR LAMPUNG
2019

Judul Skripsi : **PERLINDUNGAN HUKUM DATA PRIVASI MELALUI PENGGUNAAN TEKNOLOGI ENKRIPSI**

Nama Mahasiswa : **THANIA CHRISTY CORNE**

Nomor Pokok Mahasiswa : 1512011318

Bagian : Hukum Internasional

Fakultas : Hukum

MENYETUJUI

1. Komisi Pembimbing

Melly Aida, S.H., M.Hum.	**Rehulina, S.H., M.H.**
NIP 195910251985032014	NIP 198008122008122001

2. Ketua Bagian Hukum Internasional

Dr. Rudi Natamiharja, S.H., DEA.

NIP 197812312003121003

MENGESAHKAN

1. Tim Penguji

Ketua : **Melly Aida, S.H., M.Hum.** .....

Sekertaris/Anggota : **Rehulina, S.H., M.H.** .....

Penguji Utama : **Dr. Rudi Natamiharja, S.H., DEA.** .....

2. Dekan Fakultas Hukum

Prof. Dr. Maroni, S.H., M.Hum.

NIP 19600310 198703 1 002

Tanggal Lulus Ujian Skripsi: **19 Agustus 2019**

PERNYATAAN

Yang bertanda tangan di bawah ini:

Nama	:	Thania Christy Corne
NPM	:	1512011318
Jurusan	:	Hukum Internasional
Fakultas	:	Hukum

Dengan ini menyatakan bahwa skripsi saya yang berjudul **"Perlindungan Hukum Data Privasi melalui Penggunaan Teknologi Enkripsi"** adalah benar-benar hasil karya sendiri dan bukan hasil plagiat sebagaimana telah diatur dalam Pasal 27 Peraturan Akademik Universitas Lampung dengan Surat Keputusan Rektor Nomor 3187/H26/DT/2010.

Bandar Lampung, 21 Agustus 2019

METERAI TEMPEL
TGL. 20
C025DAFF932800023
6000
ENAM RIBU RUPIAH

Thania Christy Corne

NPM 1512011318

RIWAYAT HIDUP

Thania Christy Corne lahir di Bandar Lampung pada tanggal 27 Mei 1997 sebagai anak kedua dari tiga bersaudara, dari bapak Rony Corne dan ibu Ruwiyati. Penulis menyelesaikan pendidikan formal di Taman Kanak-kanak Dharma Wanita pada tahun 2003. Pada tahun 2003, Penulis mengemban pendidikan Sekolah Dasar di SD Negeri 1 Hanura dan menyelesaikan Pendidikan Sekolah Dasar pada tahun 2009, selanjutnya penulis mengemban Sekolah Menengah Pertama di SMP Negeri 1 Padang Cermin dan selesai pada tahun 2012 dan penulis mengemban Sekolah Menengah Atas di SMA Negeri 1 Padang Cermin dan selesai pada tahun 2015.

Penulis terdaftar sebagai mahasiswa di Fakultas Hukum Universitas Lampung pada tahun 2015. Selama menjadi mahasiswa, penulis aktif dalam organisasi Himpunan Mahasiswa Hukum Internasional Fakultas Hukum Universitas Lampung tahun 2017-2018.

PERSEMBAHAN

Puji syukur kepada Tuhan Yesus Kristus, atas kasih karunia dan anugerah-Nya, maka dengan ketulusan dan kerendahan hati serta perjuangan dan kerja keras yang telah diberikan, penulis mempersembahkan karya ilmiah ini kepada:

Kedua orang tua kandung, Papa (Rony Corne) Mama (Ruwiyati) dan kakak adikku (Maria Gracesia A. dan Kezia Veronica Corne) serta orang tua angkat, Appa (Park Myeong Soo) Emma (Kang Mi Sook) dan kedua saudaraku (Park Eun Ha dan Park Eun Chong) yang senantiasa memberikan dukungan semangat, motivasi, finansial dan nasihat serta doa yang selalu menjadi kekuatan bagi penulis untuk menyelesaikan karya ilmiah ini.

Keluarga dan sahabat yang senantiasa memberikan dukungan yang memotivasi penulisan dan almamater ku yang tercinta....

Universitas Lampung

MOTTO

"Do not worry about anything: instead pray about everything. Tell God what you need and thank Him for all he has done"

(Philippians 4:6)

"She is clothed in strength and dignity, and she laughs without fear of the future"

(Proverbs 31:25)

"JUST DO IT!"

(Sonbae)

"I get knocked down and get right back up, being strong is the ONLY choice I have"

(Penulis)

SANWACANA

Puji syukur penulis panjatkan atas kehadirat Tuhan Yang Maha Esa, karena atas berkat dan kasih-Nya karya ilmiah ini dapat diselesaikan dengan baik. Karya ilmiah berjudul "***Perlindungan Hukum Data Privasi melalui Penggunaan Teknologi Enkripsi***" sebagai salah satu syarat untuk memperoleh gelar sarjana di Fakultas Hukum Universitas Lampung.

Penyelesaian karya ilmiah ini tidak lepas dari bantuan, partisipasi, bimbingan, kerja sama dan doa dari berbagai pihak, baik secara langsung maupun tidak langsung, sehingga pada kesempatan ini, penulis mengucapkan terima kasih kepada:

1. Bapak Prof. Dr. Maroni, S.H., M.Hum. selaku Dekan Fakultas Hukum Universitas Lampung;
2. Bapak Dr. Rudi Natamiharja, S.H., DEA., selaku Ketua Bagian Hukum Internasional dan Bapak Bayu Sujadmiko, S.H., M.H., Ph.D., selaku Sekretaris Bagian Hukum Internasional;
3. Ibu Melly Aida, S.H., M.Hum., selaku Pembimbing Utama, terima kasih atas kesediaannya meluangkan waktu, tenaga dan pikirannya untuk memberikan bimbingan, saran dan kritik dalam proses penyelesaian karya ilmiah ini sehingga karya ilmiah ini dapat terselesaikan dengan sangat baik;
4. Ibu Rehulina, S.H., M.H., selaku Pembimbing Kedua, terima kasih atas kesediaannya meluangkan waktu, tenaga dan pikirannya untuk memberikan

bimbingan, saran dan kritik dalam proses penyelesaian karya ilmiah ini serta semangat dan motivasi sehingga karya ilmiah ini dapat diselesaikan dengan sangat baik;

5. Bapak Rudi Natamiharja, S.H., DEA, Ibu Desy Churul Aini, S.H., M.H., Bapak Bayu Sujadmiko, S.H., M.H., Ph.D., selaku Penguji, terima kasih atas kesediaannya meluangkan waktu, tenaga dan pikirannya untuk memberikan bimbingan, saran dan kritik dalam proses penyelesaian karya ilmiah ini;
6. Bapak Ahmad Saleh, S.H., M.H, selaku Pembimbing Akademik yang telah membantu penulis menempuh pendidikan di Fakultas Hukum Universitas Lampung;
7. Bapak/Ibu Dosen dan seluruh Staf Administrasi Fakultas Hukum khususnya bagian Hukum Internasional, terima kasih atas motivasi dan bimbingannya dalam proses penyelesaian karya ilmiah ini dan memberikan banyak ilmu pengetahuan selama menyelesaikan studi;
8. Papa, Mama, Appa dan Emma yang menjadi orang tua terhebat yang tanpa lelah memberikan kasih sayang, doa, semangat serta dukungan untuk kebahagiaan dan kesuksesan, semoga kelak dapat kembali memberikan kebahagiaan dan dapat selalu membanggakan;
9. Seluruh keluarga besar, terima kasih selalu memberikan dukungan dan motivasi dalam penyelesaian karya ilmiah ini;
10. Sonbae, *a little bit of crazy, a little bit of loud, and a whole lot of love. Thank you for always being my energy system. Thanks for the combination of love, trust, respect, and friendship. The memories of togetherness, forgiveness of mistakes and a promise to never give up are the formula of our joy.;*

11. Pablo Eduardo Garcia Juarez, *someone who always has the night while I have my day. He told me that "people always lie, but maybe it was for something." Gracias por el tiempo que siempre está disponible para brindar apoyo y recordar que siempre habrá un momento para todo. Si nuestro destino no es estar juntos, te doy gracias por regalarme un poco de tu historia.*;
12. Miftah Ramadhan, Ilham Akbar, Stefany Mindoria, Hanna Aqidatul Izzah, *some people who gave the meaning of TEAM (Together Everyone Achieve More) in my scoope. A million memories, thousands of jokes, smile and laughter shared. Anyone can find the dirt in someone, but they find the gold.*;
13. Teman-teman dan adik-adik Pengurus HIMA HI 2018-2019, terima kasih atas kebersamaan, bantuan dan motivasi dalam penyelesaian karya ilmiah ini, semoga kita semua sukses;
14. Almamaterku tercinta serta seluruh Mahasiswa Fakultas Hukum Universitas Lampung Angkatan 2015;
15. Semua pihak yang tidak dapat disebutkan satu persatu yang telah membantu dalam penyelesaian karya ilmiah ini, terima kasih atas semuanya.

Akhir kata, meskipun karya ilmiah ini masih jauh dari kata sempurna, semoga karya ilmiah ini dapat berguna dan bermanfaat bagi kita semua, Amin.

Bandar Lampung, 16 Agustus 2019

Penulis

Thania Christy Corne

DAFTAR ISI

Halaman

ABSTRAK
JUDUL DALAM
HALAMAN PERSETUJUAN
HALAMAN PENGESAHAN
RIWAYAT HIDUP
PERSEMBAHAN
MOTO
SANWACANA
DAFTAR ISI i
DAFTAR GAMBAR iii
DAFTAR TABEL iv

I. PENDAHULUAN 1
A. Latar Belakang 1
B. Rumusan Masalah 8
C. Tujuan dan Manfaat Penulisan 9
1. Tujuan Penelitian 9
2. Manfaat Penelitian 9
D. Ruang Lingkup Penelitian 10
E. Sistematika Penulisan 10

II. TINJAUAN PUSTAKA 13
A. Definisi Telekomunikasi 13
B. Definisi Data Pribadi/*Privacy* 14
C. Definisi Perlindungan Data *(Data Protection)* 16
D. Kriptografi dan Perkembangannya 20
1. Sejarah Kriptografi 22
2. Tujuan Kriptografi 25
3. Tinjauan Umum dan Konsep Dasar Kriptografi 27
3.1. Pesan, *Plainteks*, dan *Chiperteks* 27
3.2. Peserta Komunikasi 28
3.3. Kriptologi 29
E. Enkripsi dan Perkembangannya 29
F. *Law Making Treaties* dalam Perjanjian Internasional 35
G. *The OECD Guidelines for The Protection of Privacy and Transborder Flows of Personal Data* 37
H. *Amnesty International Policy on Encryption* 38
I. Ketentuan-Ketentuan terkait Penggunaan Teknologi Enkripsi dalam Perundang-undangan Indonesia 41

III. METODE PENELITIAN 46
A. Jenis Penelitian.....46
B. Pendekatan Masalah.....47
C. Sumber Data, Pengumpulan Data dan Pengolahan Data 48
1. Sumber Data 48
2. Metode Pengumpulan Data 50
3. Metode Pengolahan Data.....51
D. Analisis Data 51

IV. PEMBAHASAN DAN HASIL PENELITIAN.....53
A. Ketentuan-Ketentuan Internasional yang Berkaitan dengan Penggunaan Teknologi Enkripsi dalam Melindungi Data Privasi.....53
1. The OECD Guidelines for The Protection of Privacy and Transborder Flows of Personal Data.....53
2. Amnesty International Policy on Encryption.....62
3. Tanggung Jawab Perusahaan Teknologi Teknologi Penyedia Jasa dan Layanan Enkripsi (Pemegang Data Pribadi) untuk Menghormati Hak Asasi Manusia.....70
4. Peta Dunia Undang-Undang dan Kebijakan Enkripsi 74
B. Ketentuan-Ketentuan Indonesia yang Berkaitan dengan Penggunaan Teknologi Enkripsi dalam Melindungi Data Privasi.....133

V. PENUTUP 144
A. Kesimpulan.....144
B. Saran 146

DAFTAR PUSTAKA.....147

DAFTAR GAMBAR

Gambar 1: Skema *Public Key Encryption* 32
Gambar 2: Skema *Private Key Encryption* 34
Gambar 3: Peta Negara yang Mengatur Hak Umum Penggunaan Enkripsi 73
Gambar 4: Peta Negara-Negara dengan Pembatasan Tingkat Enkripsi ..75
Gambar 5: Peta Negara-Negara dengan Persyaratan Lisensi.....77
Gambar 6: Peta Negara-Negara dengan Pengaturan Kendali Kontrol Enkripsi 83
Gambar 7: Peta Negara-Negara dengan Pengaturan Kewajiban Perusahaan dalam Membantu Pihak Berwajib.....88
Gambar 8: Peta Negara-Negara dengan Pengaturan Kewajiban Masyarakat dalam Membantu Pihak Berwajib 115

DAFTAR TABEL

Tabel 1: Negara dengan Pengaturan Hak Umum Penggunaan Enkripsi 74
Tabel 2: Negara dengan Pembatasan Tingkat Enkripsi 76
Tabel 3: Negara-Negara dengan Persyaratan Lisensi 76
Tabel 4: Negara-Negara dengan Pengaturan Kendali Kontrol Enkripsi 83
Tabel 5: Negara-Negara dengan Pengaturan Kewajiban Perusahaan dalam Membantu Pihak Berwajib 88
Tabel 6: Negara-Negara dengan Pengaturan Kewajiban Masyarakat dalam Membantu Pihak Berwajib 116

BAB I

PENDAHULUAN

A. Latar Belakang

Keterpaduan antara perkembangan teknologi informasi dengan media dan telekomunikasi dewasa ini telah mengakibatkan semakin beragamnya aneka jasa dan produk layanan sistem informasi dan komunikasi yang ada. Dalam perkembangannya, bertemunya teknologi komputer, sistem jaringan komunikasi dan teknologi informasi melahirkan sebuah istilah yang umum digunakan di Eropa dengan nama *telematique* (telematika).[1] Sampai saat ini teknologi informasi terus-menerus berkembang tetapi penyampaiannya dan bentuknya sudah lebih modern. Teknologi informasi dan media elektronika telah mengubah perilaku masyarakat dan peradaban manusia secara global. [2]Teknologi informasi telah merubah pola hidup masyarakat secara global dan menyebabkan perubahan sosial budaya, ekonomi dan kerangka hukum yang berlangsung secara signifikan. Meskipun penetrasi internet di masyarakat internasional masih sangat kurang bila dibandingkan dengan jumlah total penduduk di dunia, akan tetapi sistem informasi dan komunikasi elektronik telah diimplementasikan pada hampir semua sektor kehidupan dalam

---

[E]Edmon Makarim, *Kompilasi Hukum Telematika*, Jakarta: PT Rajagrafindo Persada, 2005. Hlm. 4

[2] Bayu Sujadmiko, *Pengantar Hukum Teknologi Informasi Internasional*, Bandar Lampung: Zam-Zam Tower, 2017. Hlm. 1.

masyarakat. Hal ini pada akhirnya juga mengakibatkan terciptanya suatu pasar baru yang telah mendorong perkembangan sistem ekonomi masyarakat, dari ekonomi tradisional yang berbasiskan industri manufaktur ke arah ekonomi digital yang berbasiskan informasi, kreativitas, intelektual dan ilmu pengetahuan yang juga dikenal dengan istilah ekonomi kreatif.[3]

Saat ini, lebih dari tiga miliar orang di seluruh dunia memiliki akses ke internet[4]. Akses tersebut digunakan oleh berbagai pihak seperti perusahaan, rumah sakit, lembaga pendidikan dan lembaga pemerintahan. Dalam penggunaan akses internet, data privasi pengguna disimpan dan dikirim dalam basis data melalui perangkat seperti telepon genggam, tablet, komputer, dan alat elektronik lainnya.

Pemanfaatan internet dalam berbagai bidang kehidupan tidak saja membuat segala sesuatunya menjadi lebih mudah, namun juga melahirkan sejumlah permasalahan termasuk pada bidang hukum. Salah satu persoalan hukum yang terkait dengan teknologi informasi adalah data privasi, dimana teknologi internet memunginkan teraksesnya data privasi seseorang secara bebas. Hal ini terjadi karena lalu lintas pengiriman data dan informasi yang semakin global, serta konsep *open system authentification (OSA)*[5] dari suatu jaringan memudahkan seseorang untuk masuk ke dalam jaringan lainnya. Seringkali

---

[3] Edmon Makarim. *Tanggung Jawab Hukum Penyelenggara Sistem Elektronik.* Jakarta: Raja Grafindo Persada, 2010. Hal. 2.
[4] Amnesty International. *Encryption: A Matter of Human Rights.* Index: POL 40/3682/2016. 2016. Hlm. 3.
[5] Open System Authentification (OSA) adalah proses dimana komputer dapat memperoleh akses ke jaringan nirkabel yang menggunakan protocol Wired Equivalent Privacy (metode pengamanan data yang menggunakan kunci untuk autentifikasi menuju akses point).

saat seseorang hendak melakukan transaksi atau registrasi di suatu organisasi atau *mailing list* di internet, pengguna tersebut harus mengirimkan data-data pribadinya terlebih dahulu dan data ini terekam/tersimpan dalam sistem elektronik. Pada saat inilah kebocoran data terjadi dan digunakan oleh berbagai pihak seperti halnya perusahaan ataupun perseorangan. Sering terjadi bahwa pengguna internet kemudian menerima berbagai pesan iklan (untuk kemudian disebut sebagai *junk mail*) dalam kotak masuk-nya, yang kemungkinkan besar bermula dari kebocoran data pribadi yang telah diberikannya tersebut.[6] Pengiriman *junk mail* merupakan pelanggaran penggunaan data pribadi dalam bentuk yang ringan, karena seringkali data pribadi itu digunakan unuk tindak kriminal lain yang lebih berat, seperti pembobolan rekening atau pemerasan.

Disisi lain, lembaga swadaya masyarakat dewasa ini mendesak pemerintah agar dapat menindaklanjuti hak publik untuk mendapatkan akses informasi terhadap penyelenggaraan sistem pemerintahan terhadap masyarakat yang tercantum dalam Rancangan Undang-Undang (RUU) Kebebasan Informasi. Hal ini dikarenakan suatu pemerintahan yang baik dapat ditandai dengan sistem pemerintahan yang bersifat transparan *(transparancy)* dan mampu meningkatkan peran serta partisipasi publik *(publik role)* serta meningkatnya akuntabilitas publik kepada elite pemerintahnya. Sementara itu, sebenarnya juga ada hak asasi manusia yang berfungsi untuk menjaga kepentingan pribadi yakni kepentingan *privacy,* korespondensi dan harkat martabat manusia

---

[6] Asri Sitompul. *Hukum Internet, Pengenalan Mengenai Masalah Hukum Di Cyberspace,* Bandung: PT.Citra Aditya Bakti. 2001. Hal. 25.

(honor and reputation). Bahkan idealnya kepentingan publik ditujukan dalam rangka melindungi kepentingan individunya karena publik merupakan jumlah totalitas dari semua individu. Keseimbangan terhadap dua kepentingan tersebut merupakan suatu dilema dalam penegakan hukum, dimana jaminan kepentingan individu juga diselaraskan dengan kepentingan masyarakat ataupun individu lain sehingga meskipun di satu sisi ada ketentuan mengenai kebebasan informasi *(freedom of information* dan *free flow information)*, namun di sisi lain juga ada ketentuan mengenai perlindungan data *(data protection)* dan perlindungan kerahasiaan pribadi ataupun kerahasiaan informasi *(confidential information/trade secrets* ataupun *privacy protection).*

Satu contoh kasus yang menarik dari ketimpangan dalam penegakan hukum terhadap keamanan nasional dan perlindungan privasi terdapat pada kasus antara Biro Investigasi Federal Amerika Serikat/*Federal Bureau of Investigation* (*FBI*) dan Perusahaan Apple *(Apple Inc)*. Dimana pada tahun 2016, tepatnya setelah penembakan San Bernardino, *Apple* dan *FBI* melancarkan pertempuran publik atas ketersediaan enkripsi yang pada dasarnya tidak dapat dipecahkan di perangkat salah satu konsumen.[7] Hal ini terjadi karena *Apple* semakin meningkatkan penggunaan enkripsi yang tergolong kuat dan aman dalam produknya, maka ketika *FBI* berusaha membuka kode keamanan pada iPhone 5C yang digunakan oleh salah satu pelaku penembakan dalam serangan di San Bernardino, California, yang menewaskan 14 orang pada bulan Desember 2015 silam banyak menjumpai

[7] Evan Perez and Tim Hume, *"Apple Opposes Judge's Order to Hack San Bernardino Shooter's iPhone,"* CNN, February 18, 2016, diakses dari https://www.cnn.com/2016/02/16/us/san-bernerdino-shooter-phone-apple. pada tanggal 11 November 2018 pukul 17.25 WIB.

kesulitan dalam pemecahan kode keamanan tersebut sehingga hal ini menjadi penghambat bagi pihak *FBI* dalam memecahkan kasus penembakan itu. Tepat pada 16 Februari 2016, sebagai tanggapan atas permintaan dari Departemen Kehakiman Amerika Serikat, hakim-hakim federal memerintahkan Apple untuk membuat versi kustom *(backdoor*[8]*)* dari sistem operasi iOS-nya yang akan memungkinkan penyelidik dalam kasus ini untuk mendapatkan fitur keamanan ponsel. *Chief Executive Officer Apple*, Tim Cook, menanggapinya dalam sebuah surat terbuka, di mana ia menyatakan bahwa tuntutan pemerintah tersebut merupakan "pelanggaran privasi" dengan konsekuensi yang "mengerikan".

Terdapat perdebadatan di kalangan ahli teknologi, namun kebanyakan dari ahli teknologi, professor hukum, perusahaan teknologi dan organisasi hak asasi manusia mendukung kebijakan Apple dalam masalah ini.[9] Pandangan yang luas diantara mereka yang menentang permintaan FBI, adalah bahwa jika Apple dipaksa untuk memodifikasi perangkat lunaknya untuk membuka sandi ponsel tersebut akan menjadi preseden yang memungkinkan pemerintah Amerika Serikat – dan berpotensi pemerintah lainnya – serta rival perusahaan teknologi Apple untuk melemahkan atau menghalangi enkripsi mereka dengan memberikan *backdoor* bagi intelijen dan badan keamanan lainnya.

---

[8] Backdoor merupakan sebuah mekanisme untuk masuk ke dalam sistem tanpa meleewati proses proses pemeriksaan standar keamanan, seperti autentifikasi.

[9] A list of amicus briefs in support of Apple for the 22 March 2016, diakses dari http://www.usatoday.com/story/tech/news/2016/02/19/apple-fbi--court-march-22-riverside-march22/80635402/ pada tanggal 11 November 2018 pukul 20.22 WIB.

Contoh lainnya adalah kasus pembobolan *Sony Corp*, dimana pada bulan April 2011, sekelompok peretas (*hacker*) membobol jaringan *playstation Sony* dan mencuri data lebih dari 77 juta akun. Serangan ini dipercaya sebagai serangan terbesar dalam sejarah internet sehingga membuat *Sony* menutup *Playstation Network*. Akibat pembobolan itu, perusahaan memperkirakan akan kehilangan keuntungan hingga Rp 1,45 triliun. Sebagai kompensasi *Sony* telah menawarkan insentif bagi pengguna *PlayStation Network* untuk kembali ke sistem mereka setelah terjadinya serangan peretasan tersebut.[10]

Sedangkan menurut Data Norton Report 2013 menyebutkan bahwa tingkat potensi dan resiko tindak kejahatan *cyber* di Indonesia sudah memasuki status darurat. Menurut situs Id-SIRTII//CC (*Indonesia Security Incident Response Team on Internet Infrastructure/ Coordination Center*), angka *cyber crime* di tahun 2013 lalu terus menunjukkan peningkatan. Laporan tersebut menyatakan bahwa kejahatan komputer berada pada puncaknya di tahun 2013, hal ini ditandai dengan angka kasus-kasus pelanggaran keamanan pengguna kartu kredit dan debit yang mencapai jumlah hingga lebih dari 40 juta jiwa. Tidak hanya itu, serangan-serangan terhadap situs jejaring sosial pun ikut meningkat. *Data Breach Investigation* mencatat ada 50 perusahaan dan organisasi yang mendapatkan serangan *cyber* dan mencakup lebih dari 63 ribu insiden pelanggaran keamanan komputer, dan dari jumlah itu setidaknya mencakup lebih dari 95 negara.[11] Mayoritas serangan tersebut hadir dalam bentuk

---

[10] *Jaringan Sony Dibobol Lagi Jutaan Data Dicuri*, diakses dalam http://www.tempo.co/read/news/2011/06/03/07233_8366/. Pada 27 Maret 2019.

[11] Diakses dalam http://www.idsirtii.or.id/berita/baca/41/setahun-40-juta-konsumen-jadi-korban-hacking-.html. pada 31 Maret 2019

malware ataupun *phishing* dan lebih menyasar pada institusi perbankan dan pemerintahan. *Phishing* adalah usaha untuk mendapatkan suatu informasi penting dan rahasia secara tidak sah, seperti *User ID, Password,* PIN, informasi rekening bank, informasi kartu kredit, atau informasi rahasia lainnya. Istilah *phishing* sendiri berasal dari bahasa Inggris yaitu *fishing* (memancing), yang dalam hal ini berarti memancing informasi rahasia dari orang lain. *Phising* merupakan salah satu kejahatan di dunia maya *(cyber crime)* yang sering terjadi.

Tiga contoh kasus di atas merupakan contoh atas bagaimana teknologi baru dengan pemasangan enkripsi menjadi hal yang sangat penting dalam melindungi kerahasiaan data, namun demikian, hal ini juga telah menciptakan tantangan yang baru juga bagi lembaga penegak hukum, badan keamanan nasional, dan pembuat kebijakan lainnya. Menanggapi tantangan teknologi ini, pembuat kebijakan semakin mempertimbangkan kebijakan dengan dampak langsung dan tidak langsung pada efektivitas teknologi enkripsi. Ketersediaan dan penggunaan enkripsi terus mengarah pada perdebatan kebijakan hukum yang penting, rumit dan sangat kontroversial. Putaran pertama debat dengan disertai bentuk-bentuk kontestasi legal ditingkat nasional dan internasional terjadi pada tahun 1990-an. Saat ini, dunia ada dalam era putaran kedua diawali dengan akses pemerintah terhadap informasi dan komunikasi. Enkripsi yang kuat umumnya diterima sebagai bagian yang penting dan positif dari bidang media dan komunikasi. Enkripsi memainkan peranan yang sangat vital

dalam kerangka kebijakan yang mempromosikan keamanan dan integritas jaringan.

Di era digital seperti saat ini, penggunaan enkripsi merupakan bagian dari perlindungan data privasi. Hal ini dikarenakan teknologi enkripsi dapat melindungi komunikasi dan data dari tindakan memata-matai *(spying)*. Namun disayangkan, banyak pemerintah sangat kritis terhadap enkripsi dan telah membuat kebijakan serta tindakan hukum dalam mencegah atau membatasi kemampuan individu untuk menggunakan enkripsi. Negara-negara seperti Pakistan, India dan Kuba melarang enkripsi. Pejabat pemerintah, termasuk di Perancis, Inggris dan Amerika Serikat, telah mengkritik enkripsi atas kekhawatiran bahwa hal itu akan menyebabkan tim inteligen *"going dark"*[12]. Ini merupakan fakta bahwa pengguaan atas sistem enkripsi yang kuat dapat menimbulkan tantangan untuk mengakses informasi yang bertujuan untuk penegakan hukum.

B. Rumusan Masalah

Berdasarkan uraian latar belakang di atas, maka yang menjadi pokok permasalahan yang akan dibahas dalam penelitian ini adalah:

1. Bagaimanakah hukum internasional mengatur penggunaan atas teknologi enkripsi dalam melindungi data privasi?
2. Bagaimanakah hukum Indonesia mengatur persoalan penggunaan teknologi enkripsi sebagai alat untuk melindungi data privasi?

[12] *Going dark* yaitu istilah untuk buta, yang dalam hal ini diartikan dengan kekhawatiran bahwa bagian dari komunikasi online tidak dapat diakses oleh penegak hukum atau badan intelijen.

C. Tujuan dan Manfaat Penulisan

1. Tujuan Penelitian

Berdasarkan rumusan masalah di atas maka yang akan menjadi tujuan utama penelitian ini adalah :

1) Untuk mengetahui, memahami dan menganalisis apakah dalam hukum internasional penggunaan teknologi kriptografi dapat dikategorikan sebagai suatu hak asasi manusia dalam mencapai perlindungan privasi atas data pribadi.
2) Untuk mengetahui, memahami dan menganalisis pengaturan, penerapan serta implementasi teknologi enkripsi menurut perundang-undangan Indonesia.

2. Manfaat Penelitian

Manfaat dari penelitian ini terdiri dari dua aspek yaitu:

1) Manfaat Teoritis

   Hasil dari penelitian ini diharapkan dapat memberikan sumbangan pemikiran, pengetahuan dan wawasan dari penulis kepada pembaca, khususnya mengenai teknologi enkripsi yang saat ini sedang diperdebatkan eksistensinya sebagai suatu hak dalam mencapai perlindungan privasi atas data pribadi.

2) Manfaat Praktis

Hasil dari penelitian ini diharapkan dapat memberi manfaat bagi masyarakat pada umumnya, khususnya bagi para akademisi dalam mengembangkan ilmu hukum internasional pada persoalan perlindungan data privasi melalui teknologi enkripsi yang kemudian dapat digunakan sebagai data sekunder dalam melakukan penelitian lebih lanjut terkait dengan pengaturan, penerapan serta implementasi teknologi enkripsi.

D. Ruang Lingkup Penelitian

Ruang lingkup dari penelitian ini adalah perlindungan data privasi melalui teknologi enkripsi.

E. Sistematika Penulisan

Sistematika penulisan pada skripsi ini terdiri dari 5 bab yang terorganisir ke dalam bab demi bab sebagai berikut:

BAB I. Pendahuluan

Pada bab ini akan diuraikan mengenai latar belakang masalah, identifikasi masalah, ruang lingkup penelitian, tujuan dan manfaat penelitian serta sistematika penulisan. Bab ini merupakan gambaran umum dari isi skripsi untuk memudahkan pembaca dalam mempelajari dan memahami isi skripsi.

BAB II. Tinjauan Pustaka

Bab ini berisi landasan teori dan data-data yang terkait dengan skripsi, dimana akan dibahas mengenai pengertian umum perlindungan data, kriptografi, enkripsi, serta pengaturan atas penggunaan teknologi enkripsi yang diatur dalam *The OECD Guidelines for The Protection of Privacy and Transborder Flows of Personal Data*, *Amnesty International Policy on Encryption*, dan berbagai peraturan perundang-undangan nasional.

BAB III. Metodologi Penelitian

Menjelaskan metode yang digunakan dalam penelitian skripsi ini, yang terdiri dari jenis penelitian, pendekatan masalah, data dan sumber data, prosedur pengumpulan data, prosedur pengolahan data dan analisis data. Bab ini juga berisikan pembentukan gambaran secara jelas tentang bagaimana penelitian ini akan dilakukan serta didukung dengan metode penelitian ilmiah.

BAB IV. Hasil Penelitian dan Analisis Data

Pada bab ini akan dipaparkan mengenai hasil penelitian dan uraian dari pembahasannya yang terdiri dari dua sub bab, yaitu pengaturan teknologi enkripsi dalam melindungi data privasi menurut hukum internasional dan pengaturan teknologi enkripsi dalam melindungi data privasi menurut hukum nasional.

BAB V. Penutup

Bab ini terdiri dari kesimpulan dan saran. Kesimpulan merupakan inti dari uraian atas pembahasan pada Bab IV. Setelah itu, dibuatlah saran berdasarkan kesimpulan yang telah dibuat yang berguna sebagai masukan dari apa yang telah diteliti dalam skripsi ini.

BAB II

TINJAUAN PUSTAKA

A. Definisi Telekomunikasi

Teknologi komunikasi merupakan basis kemajuan teknologi manusia modern. Mulai dari 1837 ketika Samuel F. B. Morse menemukan telegraf hingga penemuan telepon genggam pertama pada tahun 1973 oleh Martin Cooper, teknologi perangkat telekomunikasi sudah berkembang setidaknya sejak dua abad terakhir.[13] Peranan teknologi telekomunikasi dalam kehidupan manusia sangat penting, hal itulah yang terus mendorong kemajuan teknologi komunikasi dan munculnya inovasi perangkat-perangkat telekomunikasi baru seiring dengan kebutuhan manusia yang semakin kompleks.

Secara teknis, proses bertelekomunikasi dilakukan dengan memancarkan *(transmission)* suatu pesan atau data dengan signal elektronik dari suatu tempat si pengirim *(origin)* dan ke suatu tempat si penerima informasi *(destination)*, baik melalui suatu medium kabel maupun melalui jalur gelombang radio *(radio link)* ataupun signal radio *(radio signal)*. Sebagai

[13] Jones, S., Kovac, R., & Groom F. M. *Introduction to Communication Technologies: A Guide for Non Engineers.* 2009. Bocaraton, FL: CRC Press. Hlm. 47.

suatu catatan , umumnya dikenal ada empat jenis sistem komunikasi elektronik, yaitu sistem komunikasi radio, sistem komunikasi satelit, sistem komunikasi telegraf, dan sistem komunikasi telepon.[14]

Secara etimologi telekomunikasi berasal dari kata "tele" yang berarti jauh dan "komunikasi" yang berarti proses pertukaran informasi individu melalui symbol bersama.[15] Lebih lanjut, sesuai dengan Pasal 1 ayat (1) Undang-undang Republik Indonesia No. 36 Tahun 1999 tentang Telekomunikasi menuliskan bahwa telekomunikasi adalah setiap pemancaran, pengiriman, dan atau penerimaan dari setiap informasi dalam bentuk tanda-tanda. Isyarat tulisan, gambar, suara dan bunyi melalui sistem kawat, optik, radio atau sistem elektromagnetik lainnya.

B. Definisi Data Pribadi / *Privacy*

Privasi merupakan suatu konsep yang sangat sulit untuk didefinisikan karena setiap orang akan memberi batasan yang berbeda tergantung dari sisi mana orang akan menilainya. Konsep privasi untuk pertama kalinya dikembangkan oleh Warren dan Brandheis yang menulis sebuah artikel di dalam jurnal ilmiah Sekolah Hukum Universitas Harvard yang berjudul *"The Right to Privacy"* atau hak untuk tidak diganggu. Dalam jurnal tersebut menurut Warren dan Brandheis dengan adanya perkembangan dan kemajuan teknologi maka timbul suatu kesadaran masyarakat bahwa telah lahir suatu kesadaran bahwa ada hak seseorang untuk menikmati hidup.

---

[14] *Opcit.* Edmon Makarim, *Kompilasi Hukum Telematika. 2004. Hlm. 110.*

[15] Danrivsnto Budhijanto, *Hukum Telekomunikasi, Penyiaran & Teknologi Informasi, Regulasi & Konvergensi*, Bandung: Refika Aditama, 2010. Hlm. 4.

Hak untuk menikmati hidup tersebut diartikan sebagai hak seseorang untuk tidak diganggu kehidupan pribadinya baik oleh orang lain, atau oleh negara. Oleh karena itu hukum harus mengakui dan melindungi hak privasi tersebut.[16] Pasal 12 *the Universal Declaaration of Human Right* dan Pasal 17 *the International Covenant on Civil and Political Rights* menjelaskan bahwa tidak seorang pun akan tunduk pada campur tangan sewenang-wenang dengan privasi, keluarga, rumah atau korespondensi, atau serangan terhadap kehormatan dan reputasinya.

Istilah perlindungan data pertama kali digunakan di Jerman dan Swedia pada tahun 1970-an yang mengatur perlindungan data pribadi melalui undang-undang. Alasan dibuatnya perlindungan karena pada waktu itu mulai dipergunakan komputer sebagai alat untuk menyimpan data penduduk, terutama untuk keperluan sensus penduduk. Ternyata dalam prakteknya, telah terjadi banyak pelanggaran yang dilakukan baik oleh pemerintah maupun pihak swasta. Karena itu agar penggunaan data pribadi tidak disalahgunakan maka diperlukan pengaturan.[17]

Tiap-tiap negara menggunakan peristilahan yang berbeda antara informasi pribadi dan data pribadi. Akan tetapi secara substantive kedua istilah tersebut mempunyai pengertian yang hampir sama sehingga kedua istilah tersebut sering digunakan bergantian. Amerika Serikat, Kanada, dan Australia menggunakan istilah informasi pribadi sedangkan negara-negara

[16] Shinta Dewi, *CyberLaw: Perlindungan Privasi atas Informasi Pribadi dalam E-Commerce menurut Hukum Internasional*, Bandung: Widya Padjajaran. 2009. Hlm. 10.
[17] *Ibid.* hlm. 37.

Uni Eropa dan Indonesia sendiri dalam UU ITE menggunakan istilah data pribadi.[18]

C. Definisi Perlindungan Data *(Data Protection)*

Privasi dan perlindungan data pribadi telah sering menjadi topik utama berita dalam beberapa tahun terakhir. Secara garis besar, data pribadi adalah segala jenis informasi (satu informasi atau sekumpulan informasi) yang dapat mengidentifikasikan individu atau menjadikannya sebagai individu. Contoh jelasnya adalah nama, alamat, nomor identitas nasional (SIM/KTP), tanggal lahir atau foto seseorang. Sedangkan beberapa contoh yang mungkin kurang jelas adalah nomor plat kendaraan, nomor kartu kredit, sidik jari, alamat Internet Protokol (IP)[19] (misalnya jika digunakan oleh seseorang di perangkatnya, seperti web server), atau catatan kesehatan. Data pribadi dinilai sangat penting bagi setiap individu karena data tersebut merupakan hal fundamental yang sangat berarti dan penting bagi kelangsungan hidup saat ini ataupun di masa depan. Oleh karena itu, perlindungan data pribadi harus diterapkan dan dikembangkan terlebih dalam sistem elektronik.

Perlindungan data tidak dapat dipisahkan dari privasi, hal ini dikarenakan data yang dilindungi merupakan privasi individu itu sendiri. Bila hendak didefinisikan, maka yang dimaksud dengan “data pribadi” adalah data

[18] *Ibid.* hlm. 71.
[19] Alamat IP adalah label numerik yang ditetapkan untuk perangkat yang terhubung ke internet.

yang berupa identitas, kode, simbol, huruf atau angka penanda personal seseorang yang bersifat pribadi.[20]

Di beberapa negara maju, masalah perlindungan data pribadi sudah dianggap sebagai bagian dari hak asasi manusia yang harus dilindungi dan oleh karenanya telah dituangkan dalam peraturan perundangan tersendiri. Sebagai contoh, selama lebih dari satu dekade, Eropa telah memiliki peraturan tentang perlindungan data pribadi.[21] Inggris mengatur tentang perlindungan data pribadi yang dituangkan ke dalam *Data Protection Act 1998* yang berlaku sejak tahun 2000. *Act* ini merupakan pengganti dari peraturan sebelumnya yaitu *Data Protection Act 1984*. Di Inggris terdapat suatu badan pelaksana perlindungan data yaitu *The Data Protection Commisioner* yang bertugas mengawasi semua pengguna data yang menguasai data pribadi. Perlindungan terhadap hak privasi individual dibuktikan dengan terbentuknya *Data Protection Act 1998* yang memungkinkan subjek data untuk mendapatkan informasi tentang pengolahan data pribadinya dan untuk mencegah beberapa jenis pengolahan data yang berlangsung bila dianggap akan membahayakan kepentingannya.[22]

---

[20] Rosalinda Elsina L, *"Aspek Hukum Perlindungan Data Pribadi di Dunia Maya"*. Gema Aktualita, Vol. 3, No. 2, 2014. Hlm 16.
[21] Gupinder Assi, *South East Asia: Data Protection Update*, www.bryancave.com/bulletins, November 2018, hlm. 1.
[22] Edmon Makarim, *Pengantar Hukum Telematika (Satu Kompilasi Kajian)*.Jakarta: Raja Grafindo Persada, 2005, hlm. 170.

Pada era informasi abad ini, teknologi informasi dan komunikasi atau ICT (*Information and Communication Technology*) telah menjadi bagian yang tidak dapat terpisahkan dari kehidupan global. Kemudahan serta keterjangkauan reformasi teknologi komunikasi mempermudah proses interaksi manusia. Dalam hal ini, saat pengguna aplikasi berbasis komunikasi memakai layanan yang disediakan oleh penyelenggara, maka untuk dapat mengakses dan menggunakan aplikasi tersebut terlebih dahulu pengguna akan melengkapi data-data pribadi sebagai salah satu syarat pembuatan akun, tidak hanya untuk registrasi awal, data juga akan secara otomatis terdapat dalam ruang komunikasi aplikasi tersebut yang dalam hal ini sering disebut sebagai metadata.

Metadata pada dasarnya berisikan semua informasi yang dihasilkan melalui penggunaan teknologi komunikasi selain konten yang sebenarnya dari sebuah komunikasi. Meskipun informasi yang disajikan tidak selalu detail pribadi atau langsung merujuk kepada kontennya, namun informasi tersebut berisikan informasi tentang perangkat yang digunakan, pengguna perangkat, dan cara penggunaannya (sebagai contoh: penerima email, durasi panggilan, catatan lokasi, serta menara seluler yang digunakan). Apabila disilangkan dengan referensi sumber data lain, maka analisa metadata akan menghasilkan gambaran yang akurat mengenai semua data dan pihak yang terkait.

Pesatnya perkembangan teknologi komputer harus diikuti dengan peningkatan sistem keamanan yang melindungi sistem komputer. Hal ini dikarenakan perkembangan teknologi komputer senantiasa diikuti dengan perkembangan teknologi untuk merusak sistem komputer baik itu pembajakan, penyusupan, perusakan sistem dan sebagainyanya. Ada aspek penting yang perlu dijaga dalam suatu sistem komputer, yaitu keamanan data dan keamanan jaringan. Keamanan data dipergunakan untuk melindungi data yang isi informasi dari data tersebut bersifat penting dan rahasia. Keamanan jaringan dipergunakan untuk transmisi data dalam suatu jaringan dimana isi informasi data tersebut dangat penting. Sebagai upaya dalam perlindungan data, maka aspek keamanan data diperlukan sebagai penunjang suatu sistem keamanan. Adapun aspek-aspek tersebut adalah[23]:

a. *Secrecy*

   Berhubungan dengan akses membaca data dan informasi. Data dan informasi di dalam suatu sistem komputer hanya dapat diakses dan dibaca oleh orang yang berhak.

b. *Integrity*

   Berhubungan dengan akses merubah data dan informasi. Data dan informasi yang berada dalam suatu sistem komputer hanya dapat dirubah oleh orang yang berhak.

---

[23] Heri Sutarno, *"Enkripsi Data Sistem Kriptografi Kunci Publik Menggunakan Algoritma Diophantine"*. Jurnal Pengajaran MIPA, Vol. 10, No. 2. 2 Desember 2007. Hlm. 9.

c. *Availability*

Berhubungan dengan ketersediaan data dan informasi. Data dan informasi yang berada dalam suatu sistem komputer dapat dimanfaatkan oleh orang yang berhak.

D. Kriptografi dan Perkembangannya

Kriptografi berasal dari bahasa Yunani, *"kryptos"* yang berarti tersembunyi dan *"graphein"* yang berarti tulisan. Oleh karena itu, kata kriptografi dapat diartikan sebagai frase "tulisan tersembunyi". *Request for Comments (RFC)* mendefinisikan kriptografi sebagai ilmu matematika yang berhubungan dengan trasformasi data untuk membuat artinya tidak dapat dipahami (untuk meyembunyikan maknanya), mencegahnya dari perubahan tanpa izin, atau mencegahnya dari penggunaan yang tidak sah. Jika transformasinya dapat dikembalikan, kriptografi juga bisa diartikan sebagai proses mengubah kembali data yang terenkripsi menjadi bentuk yang dapat dipahami. Artinya, kriptografi dapat diartikan sebagai proses untuk melindungi data dalam arti yang luas.[24] Menurut Florencia, "Kriptografi merupakan seni dan ilmu menyembunyikan informasi dari penerima yang tidak berhak."[25] Sedangkan menurut William, "Kriptografi berasal dari kata *Crypto* yang berarti "*hidden, secret"* dan pada bidang

[24] Rolf Oppliger, *"Contemporary Cryptography.* Boston, London: Artech House, 2005. Hlm. 1.
[25] Rahayu, Florensia. *"Cryptography: Suplemen Bahan Ajar Mata Kuliah Proteksi dan Teknik Keamanan Sistem Informasi".* Depok: Universitas Indonesia Press. 2005. Hlm. 47.

studi informatika dapat diartikan dengan studi mengenai menyembunyikan informasi atau informasi yang disembunyikan *(hiding information)*".[26]

Kamus Bahasa Inggris Oxford memberikan pengertian kriptografi sebagai berikut:

> *"sebuah teknik rahasia dalam penulisan, dengan karakter khusus, dengan menggunakan huruf dan karakter di luar bentuk aslinya, atau dengan metode-metode lain yang hanya dapat dipahami oleh pihak-pihak yang memproses kunci, juga semua hal yang ditulis dengan cara seperti ini."*
>
> *"a secret technique in writing, with special characters, using letters and characters outside the original form, or with other methods that can only be understood by those who process the key, as well as all things written in this way".*

Jadi, secara umum kriptografi dapat diartikan sebagai ilmu dan seni untuk menjaga pesan agar aman.[27] Para pelaku atau praktisi kriptografi disebut *Cryptographers.* Sebuah algoritma kriptografik *(cryptographic algorithm)*, disebut *chipper*, merupakan persamaan matematik yang digunakan untuk proses enkripsi dan dekripsi. Biasanya kedua persamaan matematik (untuk enkripsi dan dekripsi) tersebut memiliki hubungan matematis yang cukup erat. Proses yang dilakukan untuk mengamankan sebuah pesan (yang disebut *plaintext*) menjadi pesan yang tersembunyi (disebut *chipertext*) adalah enkripsi. *Chipertext* adalah pesan yang sudah tidak dapat dibaca

---

[26] William, Stallings. "*Cryptography and Network Security, Principles and Practices"*. Journal of Pearson Education, Inc. 2006. Hlm. 3.
[27] William Stallings, *"Network and Internetwork Security,"* Prentice Hall, 1995. Hlm. 8.

dengan mudah. Proses sebaliknya, untuk mengubah *chipertext* menjadi *plaintext*, disebut dekripsi.

Menezes, Oorschot dan Vanstone menyatakan bahwa kriptografi adalah suatu studi teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, otentikasi entitas dan otentikasi keaslian data. Kriptografi tidak hanya berarti penyediaan keamanan informasi, melainkan sebuah himpunan teknik-teknik.[28]

1. Sejarah Kriptografi

Secara historis ada empat kelompok yang berkontribusi terhadap perkembangan kriptografi, dimana mereka menggunakan kriptografi untuk menjamin kerahasiaan dalam komunikasi pesan penting, yaitu kalangan militer (termasuk intelijen dan mata-mata), kalangan diplomatic, penulis buku harian, dan pecinta *(lovers)*.[29] Di antara keempat kelompok ini, kalangan militer yang memberikan kontribusi paling penting karena pengiriman pesan di dalam suasana perang membutuhkan teknik enkripsi dan dekripsi yang rumit. Selain itu, Kriptografi juga digunakan untuk tujuan keamanan. Kalangan gereja pada masa awal agama Kristen menggunakan kriptografi untuk menjaga tulisan religious dari gangguan otoritas politik atau budaya yang dominan saat itu. [30] Sedangkan di India, kriptografi digunakan

[28] Menezes, Oorschot and Vanstone. *"Handbook of Applied Cryptography"*. Electrical Engineering and Computer Science Massachusetts Institute of Technology. 1996. Hlm. 4.
[29] Fred Cohen & Associates. *A Short History of Cryptography*.1995. Fred Cohen. Hlm. 1.
[30] *Ibid.* Hlm. 3.

oleh pecinta *(lovers)* untuk berkomunikasi tanpa diketahui orang. Bukti ini ditemukan di dalam buku *Kama Sutra* yang merekomendasikan wanita seharusnya mempelajari seni memahami tulisan dengan *chipper*.

Pada abab ke-17, sejarah kriptografi mencatat korban ketika ratu Skotlandia, Queen Mary, dipancung setelah surat rahasianya dari balik penjara (surat terenkripsi yang isinya rencana membunuh Ratu Elizabeth I) berhasil dipecahkan oleh seorang pemecah kode.

Pada Perang Dunia ke II, Pemerintah Nazi Jerman membuat mesin enkripsi yang dinamakan *Enigma*.[31] Mesin yang menggunakan beberapa buah *rotor* (roda berputar) ini melakukan enkripsi dengan cara yang sangat rumit. Namun *Enigma chipper* berhasil dipecahkan oleh pihak sekutu dan keberhasilan memecahkan *Enigma* sering dikatakan sebagai faktor yang memperpendek perang dunia ke-II.[32]

Dimulai dari usaha Feistel dari IBM di awal tahun 70-an dan mencapai puncaknya pada 1977 dengan pengangkatan DES *(Data Encryption Standard)* sebagai standar pemrosesan informasi federal Amerika Serikat untuk mengenkripsi informasi yang belum diklasifikasikan.[33]

---

[31] Menezes, Oorschot and Vanstone. 1996. *"Handbook of Applied Cryptography"*. Hlm. 7.
[32] R. F. Churchhouse. 2002. *"Codes and ciphers:Julius Caesar, the Enigma and the Internet"*. United Kingdom: University Press, Cambridge. Hlm. 2.
[33] Friedrich L. Bauer. *Decrypted Secrets: Methods and Maxims of Cryptography.* 1st Edition. 1997. Springer. ISBN-13: 078-3540604181.

DES merupakan mekanisme kriptografi yang paling dikenal sepanjang sejarah.

Pengembangan paling mengejutkan dalam sejarah kriptografi terjadi pada 1976 saat Diffie dan Hellman mempublikasikan *"New Directions in Cryptography".* Tulisan ini memperkenalkan konsep revolusioner kriptografi kunci publik dan juga memberikan metode baru untuk pertukaran kunci, keamanan yang berdasar pada kekuatan masalah logaritma diskret.[34] Meskipun Diffie dan Hellman tidak memiliki realisasi praktis pada ide enkripsi kunci publik saat itu, idenya sangat jelas dan menumbuhkan ketertarikan yang luas pada komunitas kriptografi.

Pada 1978 Rivest, Shamir dan Adleman menemukan rancangan enkripsi kunci publik yang sekarang disebut RSA.rancangan RSA berdasar pada masalah faktorisasi bilangan yang sulit, dan menggiatkan kembali usaha untuk menemukan metode yang lebih efisien untuk pemfaktoran. Tahun 80-an terjadi peningkatan luas di area ini, sistem RSA masih aman. Sistem lain yang merupakan rancangan kunci publik ditemukan oleh Taher ElGamal pada tahun 1984. Rancangan ini berdasar pada masalah logaritma diskret.

[34] Ariyus, Dony. *Pengantar Ilmu Kriptografi: Teori, Analisis dan Implementasi.* 2008. Yogyakarta: Penerbit ANDIOFFSET. Hlm. 14.

Salah satu kontribusi penting dari kriptografi kunci publik adalah tanda tangan digital. Pada 1991 standar internasional pertama untuk tanda tangan digital diadopsi. Standar ini berdasar pada rancangan kunci publik RSA. Pada 1994 pemerintah Amerika Serikat mengadopsi *Digital Signature Standard,* sebuah mekanisme kriptografi yang berdasar pada algoritma ElGamal.[35]

2. Tujuan Kriptografi

Adapun tujuan dari kriptografi yang juga merupakan aspek keamanan informasi adalah sebagai berikut[36]:

a) Kerahasiaan (*confidentiality*) adalah layanan yang digunakan untuk menjaga isi informasi dari semua pihak yang memiliki otoritas terhadap informasi. Ada beberapa pendekatan untuk menjaga kerahasiaan, dari pengamanan secara fisik hingga penggunaan algoritma matematika yang membuat data tidak dapat dipahami. Istilah lain yang senada dengan *confidentiality* adalah *secrecy* dan *privacy*.

b) Integritas data adalah layanan penjagaan pengubahan data dari pihak yang tidak berwenang. Untuk menjaga integritas data, sistem harus memiliki kemampuan untuk mendeteksi manipulasi pesan oleh pihak-pihak yang tidak berhak, antara lain penyisipan, penghapusan, dan pensubstitusian data lain

[35] Menezes, Oorschot and Vanstone. 1996. *Op. cit.* hlm. 2
[36] *Ibid.*

ke dalam pesan yang sebenarnya. Di dalam kriptografi, layanan ini direalisasikan dengan menggunakan tanda-tangan digital *(digital signature)*. Pesan yang telah ditandatangani menyiratkan bahwa pesan yang dikirim adalah asli.

c) Otentikasi adalah layanan yang berhubungan dengan identifikasi, baik mengidentifikasi kebenaran pihak-pihak yang berkomunikasi (*user authentication* atau *entity authentication*) maupun mengidentifikasi kebenaran sumber pesan *(data origin authentication)*. Dua pihak yang saling berkomunikasi harus dapat mengotentikasi satu sama lain sehingga ia dapat memastikan sumber pesan. Pesan yang dikirim melalui saluran komunikasi juga harus diotentikasi asalnya. Otentikasi sumber pesan secara implicit juga memberikan kepastian integritas data, sebab jika pesan telah dimodifikasi berarti sumber pesan sudah tidak benar. Oleh karena itu, layanan integritas data selalu dikombinasikan dengan layanan otentikasi sumber pesan. Di dalam kriptografi, layanan ini direalisasikan dengan menggunakan tanda tangan digital *(digital signature)*. Tanda tangan digital menyatakan sumber pesan.

d) Nirpenyangkalan *(non-repudiation)* adalah layanan untuk mencegah entitas yang berkomunikasi melakukan

penyangkalan, yaitu pengirim pesan menyangkal melakukan pengiriman atau penerima pesan menyangkal telah menerima pesan.

Tujuan dasar dari kriptografi adalah mewujudkan keempat aspek keamanan informasi tersebut dalam teori dan praktek.

3. Tinjauan Umum dan Konsep Dasar Kriptografi

Beberapa istilah yang penting untuk diketahui dalam membahas kriptografi adalah sebagai berikut:

3.1. Pesan, *Plainteks, dan Chiperteks*

Pesan *(message)* adalah data atau informasi yang dapat dibaca dan dimengerti maknanya. Nama lain untuk pesan adalah plainteks atau teks jelas *(cleartext).*[37] Pesan dapat berupa data atau informasi yang dikirim (melalui kurir, saluran telekomunikasi, dan sebagainya) atau disimpan di dalam media perekaman (kertas, *storage*, dan sebagainya). Pesan yang tersimpan tidak hanya berupa teks, tetapi juga dapat berbentuk citra *(image)*, suara/bunyi *(audio)*, dan video, atau berkas biner lainnya.

Agar pesan tidak dapat dimengerti maknanya oleh pihak lain, maka pesan perlu disandikan ke bentuk lain yang tidak dapat dipahami (enkripsi). Bentuk pesan yang tersandi disebut

[37] Bruce Schneier, 1996. *"Applied Cryptography, Second Edition: Protocols, Algorthms, and Source Code in C (cloth)"*. John Wiley & Sons, Inc. hlm. 1.

chipertext atau kriptogram. Proses pemnbalikan dimana *chipertext* kembali menjadi plaintext disebut dekripsi.

3.2. Peserta Komunikasi

a) Entitas atau peserta adalah orang atau sesuatu yang mengirim, menerima, atau memanipulasi informasi. Entitas bisa berupa orang, terminal komputer, kartu kredit, dan sebagainya. Jadi, orang bisa bertukar pesan dengan orang lainnya (contoh: Bismo berkomunikasi dengan Ilham) sedangkan di dalam jaringan komputer, mesin (komputer) berkomunikasi dengan mesin (contoh: mesin ATM berkomunikasi dengan komputer server di bank).
b) Pengirim adalah entitas dalam komunikasi yang mengirimkan informasi kepada entitas lainnya.
c) Penerima adalah entitas dalam komunikasi yang diharapkan menerima informasi.
d) Penyusup *(adversary)* adalah entitas diluar pengirim dan penerima yang mencoba untuk membobol keamanan informasi. Penyusup biasanya bertindak seolah-olah sebagai pengirim yang sah ataupun penerima yang sah.

3.3. Kriptologi

Kriptologi dapat juga diartikan sebagai seni dan ilmu untuk membuat dan memecahkan kode rahasia. Kriptologi dibagi menjadi kriptografi (seni dan ilmu membuat kode rahasia), kriptanalisis (ilmu dan seni untuk memecahkan chiperteks menjadi plainteks tanpa mengetahui kunci yang digunakan) dan steganografi (metoda menyembunyikan pesan atau data lainnya).[38]

Pelaku kriptanalisis disebut kriptanalis. Jika seorang kriptografer mentransformasikan *plainteks* menjadi *cipherteks* dengan suatu algoritma dan kunci maka sebaliknya seorang kriptanalis berusaha untuk memecahkan *ciphertext* tersebut untuk menemukan *plaintext* atau kunci.

E. Enkripsi dan Perkembangannya

Salah satu hal yang penting dalam komunikasi menggunakan komputer untuk menjamin kerahasiaan data adalah enkripsi. Enkripsi adalah sebuah proses yang melakukan perubahan sebuah kode dari yang bisa dimengerti menjadi sebuah kode yang tidak bisa dimengerti (tidak terbaca). Enkripsi dapat diartikan sebagai kode atau *chipper*. Sebuah sistem pengkodean menggunakan sebuah *table* atau kamus yang telah didefinisikan untuk mengganti kata dari informasi atau yang merupakan bagian dari informasi

[38] *Ibid.*

yang dikirim. Sebuah *chipper* menggunakan suatu algoritma yang dapat mengkodekan semua aliran data *(stream)* bit dari sebuah pesan menjadi *cryptogram* yang tidak dimengerti *(unitelligible)*. Karena teknik *cipher* merupakan suatu sistem yang telah siap untuk diautomasi, maka teknik ini digunakan dalam sistem keamanan komputer dan *network.*[39]

Dahulu saat masih banyak orang yang belum bisa membaca, menuliskan pesan rahasia dengan cara biasa sudah terbilang cukup pada masa itu. Namun tentu hal tersebut sangat tidak efektif, hingga mulailah dikembangkan skema enkripsi untuk mengubah pesan menjadi bentuk yang tidak bisa dibaca guna menjaga kerahasiaan dari pesan tersebut saat akan diantar ke tempat lain.

Pada tahun 700 SM, orang-orang Sparta menulis pesan yang sensitive pada kulit yang dililit pada sebuah tongkat yang disebut *scytale*. Saat tulisan tersebut dilepas akan menghasilkan karakter yang acak sehingga tak mampu untuk dibaca. Namun jika digunakan tongkat dengan diameter yang sama, maka kumpulan karakter acak itu bisa diuraikan kembali *(decrypt)* sehingga bisa dibaca oleh penerima.

Selain itu, orang Romawi menggunakan apa yang disebut sandi Chaesar. Enkripsi jenis ini terbilang sederhana dimana masing-masing huruf pada

[39] Jeff Connelly. *A Practical Implementation of a One-Time Pad Cryptosystem.* 2008. CPE 456.

teks digantikan oleh huruf lain yang memiliki selisih tertentu dalam alphabet.

Ada dua jenis enkripsi, yaitu:

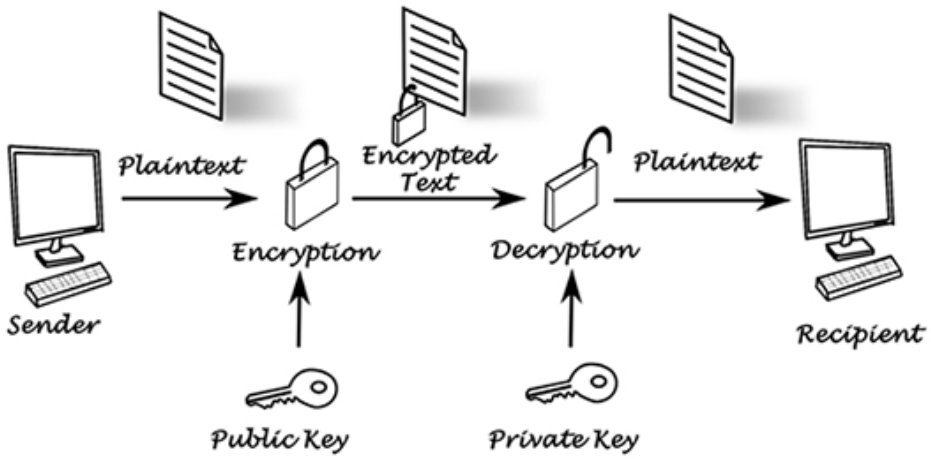
1. *Public Key Encryption* – Kunci Asimetris

   Kriptografi asimetris atau kriptografi kunci publik mempunyai banyak kelebihan, salah satunya adalah tiap orang hanya perlu memiliki satu set kunci, tanpa peduli berapa banyak orang yang akan diajak berkomunikasi.[40] Selain itu, cara enkripsi ini tidak membutuhkan saluran yang aman untuk pengiriman kunci, sebab kunci yang dikirimkan ini harus diketahui oleh publik. Cara enkripsi sangat praktis sehingga masyarakat umum pun dapat dengan mudah memakainya. Metode ini dikenal dengan nama enkripsi *publik-key* dan pertama kali diperkenalkan pada tahun 1976.

   Cara kerja enkripsi ini secara singkat dapat diterangkan sebagai berikut. Setiap orang yang menggunakan enkripsi ini harus mempunyai dua buah kunci, yang pertama disebut kunci rahasia yang hanya boleh diketahui oleh dirinya sendiri dan yang kedua disebut kunci publik yang disebarkan ke orang lain. Keduanya dibuat secara acak dengan menggunakan rumus matematika tertentu. Jadi, kedua kunci ini berkaitan erat secara matematika. Jika si A hendak mengirim pesan kepada si B,

[40] Kristanto, Andi. *Memahami Model Enkripsi dan Keamanan Data.* 2004. Yogyakarta: Andi Offset. Hlm. 9.

maka si A perlu mengenkrip pesan itu dengan kunci publik milik si B. Pesan si A yang telah dienkrip dengan menggunakan kunci puclik si B hanya bisa dibuka dengan kunci publik itu sendiri. Si B harus menjamin keamanan kunci rahasianya. Karena kuncii rahasia ini tidak perlu diketahui oleh pengirim pesan, maka kunci ini tidak akan pernah dikirim lewat jalur umum. Hal ini membuat metode enkripsi dengan kunci publik ini jauh lebih aman daripada enkripsi dengan kunci lainnya. Misalkan si C dapat mengirim pesan ke B dengan menggunakan kunci publik si B yang sama. Walaupun mengetahui kunci publik si B, pesan yang telah dienkrip dengan itu sangat sulit untuk dibuka. Cara enkripsi ini dikategorikan dalam kriptografi asimetris, karena kunci yang dipakai untuk mengenkrip dan untuk membuka enkrip (dekripsi) adalah dengan menggunakan dua kunci berbeda.[41]



Gambar 1. Skema *Public Key Encryption*

[41] Wahana komputer, dkk. 2003:94

Semua partisipan mempunyai akses ke kunci publik *(publik key)* dan kunci pribadi dihasilkan secara lokal oleh setiap partisipan sehingga tidak perlu untuk didistribusikan. Selama sistem mengontrol masing-masing *private key* dengan baik, maka komunikasi dapat dijamin keamanannya. Yang menjadi kelemahan dari metode enkripsi *publik key* adalah algoritma yang digunakan sangat komplek.

2. *Private Key Encryption* – Kunci Simetris

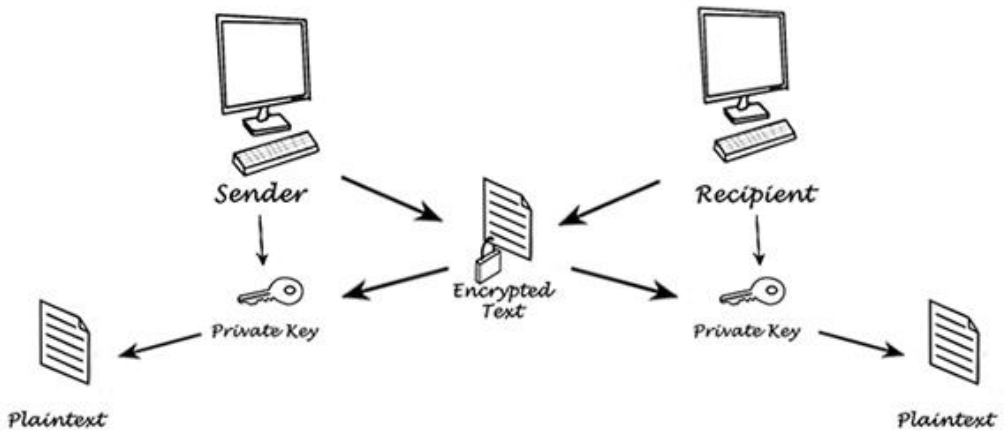
   Enkripsi dapat dilakukan jika si pengirim dan si penerima telah sepakat untuk menggunakan metode enkripsi atau kunci enkripsi tertentu. Metode enkripsi atau kuncinya ini harus dijaga ketat supaya tidak ada pihak luar yang yang mengetahuinya. Kesepakatan cara enkripsi atau kunci dalam enkripsi ini bisa dicapai lewat jalur komunikasi lain yang lebih aman, misalnya dengan bertemu langsung. Cara enkripsi dengan kesepakatan atau kunci enkripsi di atas dikenal dengan istilah enkripsi dengan kunci pribadi. Cara enkripsi inilah yang umum digunakan pada saat ini baik untuk kalangan pemerintah maupun kalangan bisnis. Cara enkripsi ini juga dikategorikan

sebagai kriptografi simetris, karena dua belah pihak mengetahui kunci yang sama.[42]

Pada kunci simetris, kunci yang digunakan untuk melakukan enkripsi dan dekripsi pada data adalah sama. Pada saat akan melakukan dekripsi, pengirim harus terlebih dahulu membagikan *private key*-nya agar bisa didekripsi oleh penerima. Kunci simetris yang paling banyak digunakan yaitu AES, yang diciptakan untuk melindungi informasi rahasia pemerintah.

Model enkripsi yang digunakan secara luas adalah model yang didasarkan pada *Data Encryption Standard (DES),* yang diambil oleh Biro Standart Nasional Amerika Serikat pada tahun 1977. Untuk *DES* data di enkripsi dalam 64 *bit block* dengan menggunakan 56 bit kunci. Dengan menggunakan kunci ini, 64 data input diubah dengan suatu urutan dari metode menjadi 64 bit output. Proses yang sama dengan kunci yang sama digunakan kembali untuk mengubah kembali enkripsi.

[42] *Ibid.* hlm. 10.



Gambar 2. Skema *Private Key Encryption*

F. *Law Making Treaties* dalam Perjanjian Internasional

Sebagai suatu sistem hukum, Hukum Internasional mempunyai beberapa sumber, seperti yang dinyatakan dalam pasal 38 ayat 1 Statuta Mahkamah Internasional, bahwa bagi Mahkamah Internasional yang tugasnya memberi keputusan sesuai dengan Hukum Internasional untuk perselisihan yang diajukan kepadanya, akan berlaku:

1. Perjanjian-perjanjian Internasional, baik yang umum maupun yang khusus, yang dengan tegas menyebutkan ketentuan-ketentuan yang diakui oleh negara-negara yang berselisih.
2. Kebiasaan-kebiasaan internasional yang terbukti merupakan praktek-praktek umum yang diterima sebagai hukum.
3. Prinsip-prinsip hukum umum yang diakui oleh bangsa-bangsa.
4. Keputusan pengadilan dan ajaran-ajaran sarjana-sarjana yang paling terkemuka dari berbagai negara sebagai sumber hukum tambahan.

Bahwa urutan-urutan sumber hukum tersebut tiga dari sumber hukum pertama yaitu 1, 2 dan 3 merupakan sumber hukum utama sedangkan sumber hukum ke 4 merupakan sumber hukum tambahan.

Pada Konferensi Wina tahun 1969 telah berhasil disepakati sebuah naskah perjanjian yang lebih dikenal dengan nama *"Viena Convention on the Law of Treaties"* atau Konvensi Wina tentang Hukum Perjanjian tahun 1969 (selanjutnya disingkat sebagai Konvensi Wina 1969). Konferensi Wina ini diadakan atas prakarsa Perserikatan Bangsa-bangsa dan naskah rancangan konvensinya disusun oleh Panitia Hukum Internasional/*International Law Commission* (yang disingkat dengan ILC), yaitu sebuah Panitia ahli dan dibentuk berdasarkan Resolusi Majelis Umum PBB No.174/II/1947[43].

Konvensi Wina tentang perjanjian ini tidak hanya sekedar merumuskan kembali atau mengkodifikasikan hukum kebiasaan internasional dalam bidang perjanjian, melainkan juga merupakan pengembangan secara progresif hukum internasional tentang perjanjian. Namun demikian Konvensi Wina ini masih tetap mengakui eksistensi hukum kebiasaan internasional tentang perjanjian, khususnya tentang persoalan-persoalan yang belum diatur dalam Konvensi Wina.

Kedudukan dari perjanjian internasional sebagai sumber hukum internasional sangat penting mengingat perjanjian internasional lebih menjamin kepastian hukum karena dibuat secara tertulis. Selain itu,

---

[43] Wayan Parthiana. *Perjanjian Internasional Tak Tertulis dalam Hukum Perjanjian Internasional.* Bandung: Mandar Maju. 1981. Hal. 344.

perjanjian internasional mengatur masalah-masalah bersama yang penting dalam hubungan antar subyek hukum internasional.

Law making treaties merupakan perjanjian internasional yang mengandung kaedah-kaedah hukum yang dapat berlaku secara universal bagi anggota-anggota masyarakat bangsa-bangsa. Saat ini pengaturan mengenai penggunaan teknologi enkripsi di dunia internasional belum terbentuk secara utuh yang dapat diberlakukan secara global. Pengaturan mengenai teknologi enkripsi hanya tertulis dalam bentuk *guidelines* yang dikeluarkan oleh organisasi internasional dan organisasi non pemerintah seperti *The Organization for Economic Co-operation and Development* dan *Amnesty International*. Oleh karena legalisasi *guidelines* hanya bersifat *soft law*, maka tidak dapat diklasifikasikan sebagai *law making treaties*, namun apabila diikuti oleh banyak negara *guidelines* ini dapat saja berubah menjadi sumber hukum internasional berupa kebiasaan internasional.

G. *The OECD Guidelines for The Protection of Privacy and Transborder Flows of Personal Data*

OECD (*Organization for Economic Co-operation and Development*) merupakan salah satu organisasi multi-nasional yang didirikan untuk memperat kerjasama dan pembangunan ekonomi antar negara demi mewujudkan stabilitas perekonomian yang berkelanjutan. OECD terdiri

dari 36[44] negara anggota yang telah membuat perjanjian multilateral terkait dengan perlindungan data privasi dalam kegiatan *e-commerce* pada konteks global *marketplace*. Rekomendasi yang dikeluarkan oleh OECD memberikan kewajiban bagi negara-negara pihak untuk membuat regulasi nasional dengan prinsip-prinsip khusus mengenai proteksi atas privasi dan kebebasan individu yang berkaitan dengan data privasi dalam jaringan yang terekam dalam *cookies* agar tidak disalahgunakan, hal ini menjadi formulasi hukum yang bersifat universal dan berlaku bagi negara-negara anggota.[45]

H. Amnesty International Policy on Encryption

Amnesty Internasional adalah organisasi non-pemerintah (NGO) yang berdiri di London pada 28 Mei 1961. Organisasi ini bertujuan untuk mempublikasikan pelanggaran oleh pemerintah ataupun entitas lain terhadap hak asasi manusia seturut dengan UDHR *(Universal Declaration of Human Rights)* yang terbentuk pada tahun 1948. Awal kemunculan organisasi *Amnesty International* dipelopori oleh ketidaksenangannya seorang pengacara bernama Peter Benenson yang marah atas dipenjarakannya dua mahasiswa Portugis yang menyuarakan kebebasan. Peter Beneson menuangkan ketidaksenangannya melalui tulisan artikel dalam Koran *The Observer*. Pada tahun 1961 Peter Beneson membuat "Amnesty 61", yang adalah merupakan sebuah kampanye yang membela

---

[44] http://www.oecd.org/about/membersandpartners/ diakses pada tanggal 8 Februari 2019 pukul 01.30 WIB

[45] Albert J. Marcella Jr. dan Carol Stucki, 2003. *Privacy Handbook: guidelines, exposures, policy implementation, and international issue*, New Jersey: John Wiley & Sons, Inc, hlm. 74.

dua mahasiswa Portugis yang dipenjara karena melakukan tos politik menggunakan gelas anggur. Tindakan yang diambil oleh Peter Benenson mendapat tanggapan yang sangat menakjubkan dari berbagai belahan dunia. Secara tidak langsung melalui artikel yang ditulis oleh Peter Benenson membuat dunia internasional disadarkan akan solidaritas dalam penegakan HAM. Kejadian ini bukan hanya melahirkan sebuah organisasi internasional namun juga awal dari perubahan sosial dunia.[46]

Pada tahun 1963, organisasi ini bergerak dalam penegakan hak asasi manusia dengan membawa misi untuk membebaskan 140 tahanan politik di dunia. Nama *Amnesty International* mulai terdengar akrab di masyarakat dunia sepanjang tahun itu. Bahkan pejabat publik dan banyak pengacara ikut dalam menyuarakan Hak Asasi Manusia atas nama *Amnesty International.* Lalu pada tahun 1965, organisasi ini mengirimkan berbagai surat untuk para tahanan politik di dunia. Surat ini berisikan dukungan terhadap mereka yang ditahan. Surat yang dikirim oleh *Amnesty International* merupakan harapan besar bagi tahanan untuk bebas. Ketika mereka bebas dari tahanan, sebagai ungkapan terima kasih merekapun ikut berjuang dalam penegakan HAM bersama *Amnesty International.*

Pada tahun 2016, tepatnya pada 22 Maret, organisasi ini mengeluarkan *research report* disertai *policy* dengan No. Index: POL40/3682/2016 yang berisi tentang enkripsi sebagai suatu bagian dari hak asasi manusia.

[46] Dikutip dari https://www.amnesty.org/en/who-we-are/ pada tanggal 24 Februari 2019 pukul 15.57 WIB.

Kebijakan ini mewakili posisi *Amnesty International* sehubungan dengan hukum hak asasi manusia internasional dan standar yang berlaku untuk penggunaan alat dan layanan enkripsi dalam teknologi digital oleh pemegang hak, dan potensi pembatasan penggunaannya oleh negara. Melalui kebijakan ini, *Amnesty International* memiliki tujuan untuk berkontribusi pada diskusi internasional dalam pemecahan masalah teknologi enkripsi. Kebijakan yang dikeluarkan oleh organisasi ini pun akan ditinjau dan direvisi sesuai kebutuhan secara berkelanjutan.

Policy on Encryption yang dikeluarkan oleh organisasi ini menjelaskan bahwa di era digital, penggunaan dan akses ke enkripsi adalah bagian penting dari hak individu untuk perlindungan privasi dan kebebasan berekspresi, informasi dan pendapat, dan juga berdampak pada hak kebebasan berkumpul, berserikat dan hak asasi manusia lainnya. Enkripsi adalah alat yang sangat penting bagi para pembela hak asasi manusia, aktivis dan jurnalis, yang semuanya bergantung padanya dengan frekuensi yang semakin meningkat untuk melindungi keamanan mereka dan orang lain. *Amnesty International* percaya bahwa negara-negara harus memfasilitasi penggunaan enkripsi dan tidak boleh mengganggu, atau mengizinkan gangguan oleh orang lain, dengan cara yang tidak dapat dibenarkan.

I. Ketentuan-Ketentuan terkait Penggunaan Teknologi Enkripsi dalam Perundang-undangan Indonesia

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik jo. Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik merupakan undang-undang yang mengatur segala hal yang berkaitan dengan teknologi informasi secara umum. Undang-undang ini sangat penting untuk dapat dipahami bagi siapapun yang terlibat dalam penggunaan teknologi informasi, baik sebagai pengguna, maupun pengembang. Hal ini dikarenakan beberapa tindakan-tindakan yang berkaitan dengan teknologi informasi didefinisikan sebagai perbuatan yang dilarang atau sering disebut dengan perbuatan melawan hukum. Lahirnya undang-undang ini disebabkan oleh globalisasi informasi yang telah menempatkan Indonesia menjadi bagian masyarakat informasi dunia. Selain itu, hadirnya undang-undang ini juga merupakan pelaksanaan atas UUD 1945 yang telah menyatakan bahwa informasi merupakan hak asasi yang dilindungi oleh undang-undang. Sebagaimana yang tercantum dalam Pasal 28F:

> *"Setiap orang berhak untuk berkomunikasi dan memperoleh informasi untuk mengembangkan pribadi dan lingkungan sosialnya, serta berhak untuk mencari, memperoleh, memiliki, menyimpan, mengolah, dan menyampaikan informasi dengan menggunakan segala jenis saluran yang tersedia."*

Meskipun setiap warga negara memiliki hak dan kebebasan dalam menggunakan informasi, UUD 1945 menyatakan bahwa hak tersebut

harus tetap dibatasi dalam rangka menghormati hak dan kebebasan orang lain jua. Sebagaimana tecantum dalam Pasal 28 J ayat 2

> *"Dalam menjalankan hak dan kebebasannya, setiap orang wajib tunduk kepada pembatasan yang ditetapkan dengan undang-undang dengan maksud semata-mata untuk menjamin serta penghormatan atas hak dan kebebasan orang lain, untuk memenuhi tuntutan yang adil sesuai dengan pertimbangan moral, nilai-nilai agama, keamanan, dan ketertiban umum dalam suatu masyarakat demokratis."*

Pengelolaan informasi merupakan sesuatu yang penting bagi negara dan menguasai hajat hidup orang banyak. Berdasarkan UUD 1945, hal ini perlu dikontrol oleh negara untuk kemaslahatan orang banyak. Dalam pasal 33 ayat 2 UUD 1945, tertulis bahwa:

> *"Cabang-cabang produksi yang penting bagi negara dan yang menguasai hajat hidup orang banyak dikuasai oleh negara."*

UU ITE secara eksplisit menyebutkan perbuatan-perbuatan terlarang mengenai informasi dan transaksi elektronik. Adapun beberapa contoh perbuatan yang dilarang dalam UU ITE ini adalah mengakses sistem elektronik milik orang lain dengan cara melanggar, menerobos, melampaui, atau menjebol sistem keamanan dengan tujuan untuk memperoleh informasi, serta penyadapan atas informasi dalam komputer milik orang lain, kecuali dilakukan oleh pihak khusus dengan izin khusus (seperti untuk upaya penegakan hukum). Muatan dalam peraturan ini sudah cukup baik, akan tetapi belum terdapat pengaturan mengenai teknologi enkripsi yang kerap kali berperan secara vital dalam perlindungan data. Teknologi enkripsi sangat dibutuhkan dalam menjamin keamanan data yang dimiliki setiap individu maupun lembaga untuk

menjaga kerahasiaannya. Dalam UU ITE ini, kegiatan penyadapan (intersepsi) dilegalkan dengan dalih sebagai upaya penegakan hukum, yang tentunya hanya dapat dilakukan oleh badan khusus yang sudah memegang izin khusus untuk melakukannya.

Sementara itu, penyadapan (intersepsi) belum diatur secara khusus dalam undang-undang. Pengaturannya tersebar dalam berbagai undang-undang.

Beberapa regulasi (perundangan-undangan) yang mengatur tentang penyadapan/intersepsi dapat dilihat dalam: Pasal 1 angka 19, Pasal 75 huruf i, Pasal 77 Undang-Undang Nomor 35 Tahun 2009 tentang Narkotika. Pengaturan penyadapan dalam UU Narkotika ini termasuk dalam UU KPK yang cukup detil mengatur penyadapan dibandingkan dengan undang-undang lainnya. Namun saja tetap memiliki sejumlah kelemahan, karena berpotensi disalahgunakan karena tata cara penyadapannya diatur secara berbeda-beda. Aturan lainnya juga terdapat di dalam Pasal 40 dan Pasal 42 Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi.

Pasal 26 Undang-Undang Nomor 31 Tahun 1999 jo. Undang-Undang Nomor 20 Tahun 2001 tentang Pemberantasan Tindak Pidana Korupsi, juga mengatur tentang penyadapan termasuk kewenangan KPK yang melakukan penyadapan di dalam Pasal 12 huruf a jo. Pasal 6 huruf c Undang-Undang Nomor 30 Tahun 2002 tentang Komisi Pemberantasan Korupsi, Pasal 31 Undang-Undang Nomor 15 Tahun 2003 tentang Penetapan Perpu Nomor 1 Tahun 2002 tentang Pembereantasan Tindak

Pidana Terorisme menjadi Undang-Undang, yang juga diatur tentang penyadapan yakni Pasal 19 ayat (2) Undang-Undang Nomor 18 Tahun 2003 tentang Advokat.

Aturan lainnya yakni Pasal 31 Undang-Undang Nomor 21 Tahun 2007 tentang Pemberantasan Tindak Pidana Perdagangan Orang, Pasal 31, Pasal 32, Pasal 47 Undang-Undang Nomor 17 Tahun 2011 tentang Intelijen Negara mengatur mengenai kewenangan untuk melakukan penyadapan oleh Badan Intelijen Negara (BIN).

Pasal 20 ayat (3) Undang-Undang Nomor 18 Tahun 2011 tentang Perubahan atas Undang-Undang Nomor 22 Tahun 2004 tentang Komisi Yudisial ini mengatur mengenai ketentuan bahwa Komisi Yudisial (KY) dapat meminta bantuan kepada aparat penegak hukum untuk melakukan penyadapan dan merekam pembicaraan dalam hal adanya dugaan pelanggaran Kode Etik dan/atau Pedoman Perilaku Hakim oleh Hakim.

Pengaturan penyadapan (intersepsi) juga terdapat di dalam perundang-undangan lainnya, seperti dalam Peraturan Pemerintah Nomor 19 Tahun 2000 tentang Tim Gabungan Pemberantasan Tindak Pidana Korupsi. Secara tegas terdapat dalam Pasal 87, Pasal 88, Pasal 89. Aturan lainnya yakni Peraturan Pemerintah Nomor 52 Tahun 2000 tentang Penyelenggaraan Telekomunikasi, Permenkominfo Nomor 11 Tahun 2006 tentang Teknis Penyadapan terhadap Informasi, Permenkominfo Nomor 1 Tahun 2008 tentang Perekaman Informasi untuk Pertahanan dan Keamanan Negara, Perkapolri Nomor 5 Tahun 2010 tentang Tata Cara

Penyadapan pada Pusat Pemantauan Kepolisian Negara Republik Indonesia, dan Standar Operasional Prosedur KPK yang sifatnya sangat rahasia.

BAB III

METODE PENELITIAN

A. Jenis Penelitian

Penelitian merupakan suatu sarana pokok dalam pengembangan ilmu pengetahuan maupun teknologi. Penelitian memiliki tujuan untuk mengungkapkan kebenaran secara sistematis, metodelogis dan konsisten, termasuk penelitian hukum. Penelitian hukum berbeda dengan penelitian sosial karena hukum tidak termasuk kategori ilmu sosial. Ilmu hukum adalah *sui generis*[47], artinya hukum merupakan ilmu jenis tersendiri. Sifat khas (*sui generis*), yang memiliki ciri (a) bersifat empiris analitis yakni memaparkan dan menganalisis terhadap isi dan struktur hukum; (b) sistematisasi gejala hukum; (c) melakukan interpretasi terhadap substansi hukum yang berlaku, serta (e) arti praktis ilmu hukum berkaitan erat dengan dimensi normatifnya.[48] Karena ini pula metode penelitiannya pun berbeda dengan penelitian sosial pada umumnya. Dalam penyusunan skripsi ini, jenis penelitian yang digunakan adalah yuridis normatif. Penelitian yuridis normatif adalah penelitian yang dilakukan dengan tujuan

---

[47] Philipus M. Hadjon, Tatik Sri Djatmiati, *Argumentasi Hukum,* Gajah Mada University Press, Yogyakarta, 2005, hlm.1.

[48] DHM Meuwissen, *Pengembangan Hukum, Pro Justicia,* Universitas Parahiyangan, Th.XII, No. 1, Januari 1994, hlm. 61-65 dalam Herowati Poesoko, *Parate Executie – Obyek Hak Tanggungan,* Laksbang Presindo, Yogyakarta, 2007, hlm. 27.

untuk menemukan aturan hukum, prinsip-prinsip hukum maupun doktrin-doktrin hukum guna menjawab isu hukum yang dihadapi[49] atau isu hukum dalam konsistensinya dengan asas-asas hukum yang ada.

B. Pendekatan Masalah

Pendekatan masalah merupakan proses pemecahan atau penyelesaian masalah melalui tahap-tahap yang telah ditentukan sehingga mencapai tujuan. Pendekatan tersebut dimaksudkan agar pembahasan dapat terfokus pada permasalahan. Sesuai dengan tujuan yang akan dicapai, maka metodologi dalam penelitian skripsi ini menggunakan tiga macam pendekatan, yakni Pendekatan Peraturan Perundang-undangan *(Statute Approach)*, Pendekatan Konseptual *(Conceptual Approach)*, serta pendekatan Kasus *(Case Approach)*.[50] Pendekatan Peraturan Perundang-undangan *(Statute Approach)* merupakan pendekatan yang dilakukan dengan menelaah semua peraturan dan undang-undang dengan peraturan dan undang-undang lainnya, baik di tingkat internasional maupun nasional. Pendekatan demikian merupakan cara untuk menemukan konsistensi pengaturan menyangkut penggunaan teknologi enkripsi yang merupakan sarana atas perlindungan hak privasi dan kebebasan berekspresi. Pendekatan Konseptual *(Conseptual Approach)* dilakukan dengan harapan ditemukan konsep-konsep baru seiring dengan dinamika dan perubahan sosial yang terjadi untuk menjawab isu hukum penelitian. Sedangkan pendekatan kasus dilakukan untuk menjaring preseden berupa

[49] Peter Mahmud Marzuki, *Penelitian Hukum*, Prenada Media, Jakarta, 2005, hlm. 29-36.
[50] Ibid, hlm. 93.

putusan pengadilan yang berkaitan dengan "*Lawful Hacking"* sebagai dasar upaya penegakan hukum. Berdasarkan tiga pendekatan tersebut diharapkan dapat diperoleh kedalaman analisa baik dari aspek norma yang sedang berlaku, konsep-konsep yang terus berkembang hingga putusan pengadilan sehingga hasil penelitian ini nanti dapat melahirkan preskripsi yang menyeluruh.

C. Sumber Data, Pengumpulan Data dan Pengolahan Data

1. Sumber Data

Penelitian ini mengunakan sumberdata sekunder yang terdiri atas sumber bahan hukum primer, sekunder dan tersier. Pertama, sumber bahan hukum primer adalah bahan hukum yang bersifat autoritatif artinya memiliki otoritas yang terdiri atas peraturan perundang-undangan, catatan resmi atau risalah dalam pembuatan peraturan perundang-undangan, atau putusan pengadilan. Sumber bahan hukum primer pada skripsi ini antara lain:

a. *The OECD Guidelines for The Protection of Privacy and Transborder Flows of Personal Data;*

b. *Amnesty International Policy on Encryption;*

c. *UN Guiding Principles on Business and Human Rights (UNGPs)*

d. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik jo. Undang-Undang Nomor 19 Tahun 2016

tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik;

e. Undang-Undang Nomor 35 Tahun 2009 tentang Narkotika;

f. Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi;

g. Undang-Undang Nomor 31 Tahun 1999 jo. Undang-Undang Nomor 20 Tahun 2001 tentang Pemberantasan Tindak Pidana Korupsi;

h. Undang-Undang Nomor 30 Tahun 2002 tentang Komisi Pemberantasan Korupsi;

i. Undang-Undang Nomor 15 Tahun 2003 tentang Penetapan Perpu Nomor 1 Tahun 2002 tentang Pemberantasan Tindak Pidana Terorisme menjadi Undang-Undang;

j. Undang-Undang Nomor 18 Tahun 2003 tentang Advokat;

k. Undang-Undang Nomor 21 Tahun 2007 tentang Pemberantasan Tindak Pidana Perdagangan Orang;

l. Undang-Undang Nomor 18 Tahun 2011 tentang Perubahan atas Undang-Undang Nomor 22 Tahun 2004 tentang Komisi Yudisial;

m. Peraturan Pemerintah Nomor 19 Tahun 2000 tentang Tim Gabungan Pemberantasan Tindak Pidana Korupsi;

n. Peraturan Pemerintah Nomor 52 Tahun 2000 tentng Penyelenggaraan Telekomunikasi;

o. Permen Kominfo Nomor 11 Tahun 2006 tentang Teknis Penyadapan terhadap Informasi;

p. Permen Kominfo Nomor 1 Tahun 2008 tentang Perekaman Informasi untuk Pertahanan dan Keamanan Negara.

q. Permen Kominfo Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik.

Kedua, bahan hukum sekunder, yaitu bahan hukum yang memberikan penjelasan serta pemahaman mengenai bahan hukum primer, seperti hasil penelitian, hasil karya hukum dan lain sebagainya[51] yang terdiri dari buku-buku, skripsi, artikel, jurnal, surat kabar, internet, hasil penelitian, pendapat para ahli atau sarjana hukum yang dapat mendukung pemecahan masalah dalam penelitian ini.

Ketiga, bahan hukum tersier yang terdiri dari bahan-bahan yang memberikan petunjuk maupun penjelasan terhadap bahan hukum primer dan bahan hukum sekunder, yaitu kamus dan ensiklopedia serta bahan-bahan lainnya yang menunjang data penelitian.

2. Metode Pengumpulan Data

Metode pengumpulan data yang akan diolah dalam penulisan skripsi ini adalah menggunakan teknik studi kepustakaan yaitu dengan mengumpulkan berbagai ketentuan perundang-undangan, dokumentasi, literatur, serta mengakses internet yang berkaitan dengan permasalahan dalam lingkup hukum internasional maupun lingkup hukum nasional.[52]

---

[51] Soerjono Soekanto. (2014). *Pengantar Penelitian Hukum*, Jakarta: Universitas Indonesia, hlm.52.

[52]Soerjono Soekanto & Sri Mamudji, *Penelitian Hukum Normatif Suatu Tinjauan Singkat*, Jakarta: PT Raja Grafindo Persada, 2009; hlm.41.

3. Metode Pengolahan Data

Data yang diperoleh dan telah terkumpul langkah berikutnya yang dilakukan adalah data tersebut diolah agar dapat memberikan gambaran mengenai masalah yang diajukan. Tahapan pengelolaan data dalam penulisan skripsi ini meliputi tahapan sebagai berikut:[53]

1) Identifikasi data atau seleksi data yaitu mencari data yang diperoleh untuk disesuaikan dengan pembahasan yang akan dilakukan dengan menelaah peraturan, buku atau artikel yang berkaitan dengan judul dan permasalahan dan sesuai dengan keperluan penelitian.
2) Klasifikasi data yaitu hasil identifikasi data yang selanjutnya diklasifikasi atau di kelompokan sehingga diperoleh data yang benar-benar objektif.
3) Penyusunan data atau sistematika data yaitu menyusun data menurut sistematika yang telah ditetapkan dalam penelitian sehingga memudahkan peneliti dalam menginterpretasikan data.

D. Analisis Data

Penulisan skripsi ini menggunakan bahan-bahan yang diperoleh dari tinjauan kepustakaan yang bersumber dari buku-buku dan literatur lain. Data yang telah diperoleh akan dianalisis secara normatif, yaitu membandingkan data yang diperoleh dengan aturan hukum. Metode yang digunakan dalam analisis data adalah analisis kualitatif yaitu memberikan arti dari setiap data yang diperoleh dengan cara menggambarkan atau

[53]Abdulkadir Muhammad. (2004). *Hukum dan Penelitian Hukum*. Bandung: Citra Aditya Bakti; hlm.122.

menguraikan data hasil penelitian dalam bentuk uraian kalimat secara terperinci, teratur, runtun, logis, tidak tumpang tindih dan efektif yang bertujuan untuk memudahkan interpretasi data dan analisis[54] serta kemudian ditariklah beberapa kesimpulan sebagai jawaban dari masalah yang diangkat dalam penulisan ini.

[54]*Ibid;* hlm.127.

BAB V

PENUTUP

A. Kesimpulan

Dari keseluruhan bab pada skripsi ini, maka dapat diambil kesimpulan sebagai berikut:

1. Teknologi enkripsi dinilai sangat penting dalam melindungi data privasi. Pengaturan mengenai penggunaan teknologi enkripsi dalam level internasional sudah ditetapkan di dalam *guidelines* seperti *The OECD Guidelines for The Protection of Privacy and Transborder Flows of Personal Data* dan *Amnesty International Policy on Encryption* yang memperbolehkan negara untuk mendekripsi data pribadi individu atas dasar kedaulatan, keamanan nasional dan kebijakan publik, namun sebaliknya sebagaimana yang telah ditetapkan dalam *UN Guiding Principle on Business and Human Rights* bahwa perusahaan pemegang data pribadi memiliki tanggung jawab untuk menghormati hak asasi manusia secara independen dan terlepas dari kemampuan dan kemauan negara, akan tetapi pengaturan-pengaturan tersebut belum dapat diterapkan secara global karena legalisasinya hanya bersifat *soft*

law. Pengaturan internasional mengenai teknologi enkripsi yang berlaku bagi seluruh negara-negara di dunia belum dibentuk sampai saat ini. Pengaturan mengenai teknologi enkripsi sangat penting karena masalah penggunaan layanan dan jasa teknologi enkripsi serta pendekripsiannya berkaitan erat dengan hak asasi manusia.

2. Pengaturan Indonesia yang berkenaan dengan teknologi enkripsi tidak dituliskan secara jelas penggunaannya, namun dalam beberapa perundang-undangan nasional (Narkotika; Psikotropika; Telekomunikasi; Tindak Pidana Korupsi; Tindak Pidana Terorisme; Tindak Pidana Perdagangan Orang; Informasi dan Transaksi Elektronik; Intelijen Negara; KPK; Advokat; Komisi Yudisial; dan perundang-undangan lainnya) disebutkan bahwa kegiatan penyadapan (yang merupakan lanjutan khusus berupa tindakan dekripsi atas penggunaan layanan dan jasa enkripsi) dilegalkan dengan dalih sebagai upaya penegakan hukum, yang tentunya hanya dapat dilakukan oleh badan khusus yang sudah memegang izin khusus untuk melakukannya. Diberikannya kewenangan penyadapan kepada aparat penegak hukum secara normatif tidak bertentangan dengan hak asasi manusia. Kewenangan penyadapan/dekripsi atas penggunaan teknologi enkripsi walaupun belum secara konkret dituliskan, namun telah memenuhi asas legalitas dan sesuai dengan norma dasar di dalam Pasal 28J ayat (2) UUD 1945.

B. Saran

Adapun saran yang akan disampaikan penulis dalam penulisan skripsi ini adalah bahwasanya kita perlu menyeimbangkan hak-hak individu dengan kebutuhan akan keselamatan publik dalam penggunaan teknologi enkripsi. Dalam hal ini, kepentingan pemerintah yang di dalamnya mencakup nilai keamanan nasional dan kepentingan individu terhadap perlindungan data privasi mereka harus dapat diseimbangkan dengan sebuah peraturan yang mengatur penggunaan atas teknologi enkripsi itu sendiri. Masih ada waktu bagi negara-negara untuk mengembangkan kebijakan nasional maupun internasional yang akan menciptakan keseimbangan ini. Namun ini bukan berarti kita memiliki waktu yang tidak terbatas untuk menentukan kebijakannya, seiring waktu berjalan, maka masalah yang berkaitan dengan enkripsi ini akan terus bermunculan karena semakin banyak perangkat yang terhubung ke internet *(Internet of Things/IoT)*.

DAFTAR PUSTAKA

Buku

Abdulkadir Muhammad. (2004). "*Hukum dan Penelitian Hukum"*. Bandung: Citra Aditya Bakti.

Al Wisnubroto dan G. Widiartana. (2005). *Pembaharuan Hukum Acara Pidana*, Bandung: Citra Aditya Bakti.

Albert J. Marcella Jr. dan Carol Stucki. (2003). "*Privacy Handbook: guidelines, exposures, policy implementation, and international issue*". New Jersey: John Wiley & Sons, Inc.

Ariyus, Dony. (2008). *Pengantar Ilmu Kriptografi: Teori, Analisis dan Implementasi*. Yogyakarta: Penerbit ANDIOFFSET.

Asri Sitompul. (2001). *Hukum Internet, Pengenalan Mengenai Masalah Hukum Di Cyberspace*, Bandung: PT.Citra Aditya Bakti.

Bayu Sujadmiko. (2017). *"Pengantar Hukum Teknologi Informasi Internasional"*. Bandar Lampung: Zam-Zam Tower.

Bruce Schneier. (1996). *"Applied Cryptography, Second Edition: Protocols, Algorthms, and Source Code in C (cloth)"*. John Wiley & Sons, Inc.

Danrivsnto Budhijanto. (2010). *Hukum Telekomunikasi, Penyiaran & Teknologi Informasi, Regulasi & Konvergensi*, Bandung: Refika Aditama.

Edmon Makarim. (2010). *Tanggung Jawab Hukum Penyelenggara Sistem Elektronik.* Jakarta: Raja Grafindo Persada.

Edmon Makarim. (2005). "*Pengantar Hukum Telematika (Satu Kompilasi Kajian)".* Jakarta: Raja Grafindo Persada.

Fred Cohen & Associates. *A Short History of Cryptography*.1995. Fred Cohen.

Harry Newton. (1998). *Newton's Telecom Dictionary* (New York: Flatiron Publishing, a division of Miller Freeman, Inc.,

Jeff Connelly. (2008). *A Practical Implementation of a One-Time Pad Cryptosystem*. CPE 456.

Jones, S., Kovac, R., & Groom F. M. *Introduction to Communication Technologies: A Guide for Non Engineers.* 2009. Bocaraton, FL: CRC Press.

Kristanto, Andi. (2004). *Memahami Model Enkripsi dan Keamanan Data.* Yogyakarta: Andi Offset

Menezes, Oorschot and Vanstone. (1996). *"Handbook of Applied Cryptography"*. Electrical Engineering and Computer Science Massachusetts Institute of Technology.

Peter Mahmud Marzuki. (2005). "*Penelitian Hukum".* Jakarta: Prenada Media.

Philipus M. Hadjon, Tatik Sri Djatmiati. (2005). "*Argumentasi Hukum".* Yogyakarta: Gajah Mada University Press.

Rahayu, Florensia. (2005). *"Cryptography: Suplemen Bahan Ajar Mata Kuliah Proteksi dan Teknik Keamanan Sistem Informasi".* Depok: Universitas Indonesia Press.

Rolf Oppliger. (2005). *"Contemporary Cryptography".* Boston, London: Artech House.

R. F. Churchhouse. (2002). *"Codes and ciphers:Julius Caesar, the Enigma and the Internet"*. United Kingdom: University Press, Cambridge.

Shinta Dewi. (2009). "*CyberLaw: Perlindungan Privasi atas Informasi Pribadi dalam E-Commerce menurut Hukum Internasional"*. Bandung: Widya Padjajaran.

Soerjono Soekanto. (2014). "*Pengantar Penelitian Hukum"*. Jakarta: Universitas Indonesia.

Soerjono Soekanto & Sri Mamudji. (2009). "*Penelitian Hukum Normatif Suatu Tinjauan Singkat*". Jakarta: PT Raja Grafindo Persada.

Voigt, Paul & Bussche, Axel von dem. (2017). "*The EU General Data Protection Regulation (GDPR): A Practical Guide"*. Switzerland: Springer International Publishing AG.

Wayan Parthiana. (1981). *Perjanjian Internasional Tak Tertulis dalam Hukum Perjanjian Internasional.* Bandung: Mandar Maju.

William A. Carter, (2017). *"The Effect of Encryption on Lawful Access to Communications and Data"* CSIS.

William Stallings. (1995). *"Network and Internetwork Security"* . Prentice Hall.

Jurnal dan Artikel

DHM Meuwissen. (1994). " *Pengembangan Hukum",* Pro Justicia Th.XII, No. 1, Universitas Parahiyangan.

Friedrich L. Bauer. *Decrypted Secrets: Methods and Maxims of Cryptography*. 1st Edition. 1997. Springer. ISBN-13: 078-3540604181.

Heri Sutarno. (2007). *"Enkripsi Data Sistem Kriptografi Kunci Publik Menggunakan Algoritma Diophantine"*. Jurnal Pengajaran MIPA, Vol. 10, No. 2.

Herowati Poesoko. (2007). "*Parate Executie – Obyek Hak Tanggungan"*. Yogyakarta: Laksbang Presindo.

Laudon, K.C. dan Jane P. Laudon. (2004). "*Management Information Systems".* 8th edition. New Jersey: Prentice-Hall, Inc.

Naniek Noviari. (2013). "*Pengaruh Teknologi Informasi Terhadap Perkembangan Akuntansi"*. Denpasar: FE Udayana.

Rosalinda Elsina L. (2014). *"Aspek Hukum Perlindungan Data Pribadi di Dunia Maya"*. Gema Aktualita, Vol. 3, No. 2.

Wahana komputer, dkk. 2003:94

William, Stallings. (2006). "*Cryptography and Network Security, Principles and Practices"*. Journal of Pearson Education, Inc.

Website

A list of amicus briefs in support of Apple for the 22 March 2016, http://www.usatoday.com/story/tech/news/2016/02/19/apple-fbi--court-march-22-riverside-march22/80635402/

Adhi Maulana, *Tingkat Kejahatan Cyber di Indonesia Sudah Gawat.* http://tekno.liputan6.com/read/2019078/tingkat-kejahatan-cyber-di-indonesia-sudah-gawat.

Christopher T. Cloutier and Jane Y. Cohen, *"Casting a Wide Net: China's Encryption Restrictions,"* King & Spalding LLC, dalam http://www.kslaw.com/imageserver/KSPublic/library/publication/2011articles/11-11WorldECRCloutierCohen.pdf.

Encrypted traffic comprises 50 percent to 70 percent of global internet traffic based on estimates from two sources: 70 percent-Sandvine, 2016 *Global Internet Phenomena Spotlight: Encrypted Internet Traffic* (Waterloo, ONT: Sandvine, 2016), https://www.sandvine.com/trends/encryption.html; 50 percent-Comments by Parisa Tabriz, Google Security Princess.

European Commision for Democracy Though Law, *"Federal Law of The Federal Security Service of The Russian Federation"* , termuat dalam http://www.icla.up.ac.za/images/un/use-of-force/eastern-europe/Russia/Federal%20Law%20on%20Federal%20Security%20Service%20Russia%201995.pdf

Evan Perez and Tim Hume (2016, 18 Februari) *"Apple Opposes Judge's Order to Hack San Bernardino Shooter's iPhone,"* CNN. Diakses dari https://www.cnn.com/2016/02/16/us/san-bernerdino-shooter-phone-apple/

"Govt to Withdraw Controversial Draft Encryption Policy after Backlash" Business Standard, September 22, 2015. http://www.business-standard.com/article/current-affairs/govt-to-withdraw-controversial-draft-encrypion-policy-after-backlash-115092200435_1.html

Gupinder Assi, "*South East Asia: Data Protection Update",* www.bryancave.com/bulletins/

Hon. Michael Kirby. *30th anniversary of the OECD Privacy Guidelines.* www.oecd.org/internet/interneteconomy/49710223.pdf.

James Lewis and Stewart Baker, *The Economic Impact of Cybercrime and Cyber Espionage* (Santa Clara, CA:McAfee/CSIS, 2013), http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime.pdf.

James Titcomb, *"WhatsApp Shutdown in Brazil Blocks 100 Million Users,"* Teelegraph, May 3, 2016, http://www.telegraph.co.uk/technology/2016/05/03/whatsapp-shutdown-in-brazil-blocks-100-million-users.

Jaringan Sony Dibobol Lagi Jutaan Data Dicuri, http://www.tempo.co/read/news/2011/06/03/07233_8366/

John Perry Barlow, *"A Declaration of the Independence of Cyberspace,"* Electronic Frontier Foundation, February 8, 1996. https://www.eff.org/cyberspace-indepence

Jordan Pearson and Justin Ling, *"Exclusive: How Canadian Police Intercept and Read Encrypted Blackberry Message,"* Motherboard, April 14, 2016, http://motherboard.vice.com/read/rcmp-blackberry-project-clemenza-global-encryption-key-canada.

Lahiri, Kris (2018). *"What is General Data Protection Regulation?"*. Forbes. Jersey City: Forbes Media. https://www.forbes.com/sites/quora/2018/02/14/what-is-general-data-protection-regulation/#15713a062dd8

Legi Mobile, *"Obligations des Operateurs et des Prestataires de Service"*, October 3, 2015 yang telah diterjemahkan http://legimobile.fr/fr/lr/code/securite_interieure/20151003/#sec30937374

Matthes Waxman and Doron Hindin, *"How Does Israel Regulate Encryption?"* Lawfare (blog),, November 30, 2015, https://www.lawfareblog.com/how-does-israel-regulate-encryption#.

Ministry of the Interior of France, *"Initiative franco-allemande sur la securite interieure en Europe,"* August 23, 2016, http://www.interieur.gouv.fr/Actualites/L-actu-du-Ministere/Initiative-fraco-allemande-sur-la-securite-en-Europe.

Office of the UNH High Commissioner for Human Rights, *Apple-FBI* case could have serious global ramifications for human rights: Zeid, 4 March 2016, http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=17138#sthash.o25R7Bqg.dpuf

Patrick Howell O'Neill, *"Russia Lawmakers Pass Sweeping Spying Law that Requires Encryption Backdoors, Call Surveillance,"* Daily Dot, http://www.dailydot.com/layer8/encryption-backdoor-russia-fsb-bill-passes/

Supriyadi Widodo Eddyono, *Mengatur Ulang Hukum Penyadapan Indonesia*. ICJR. 2009. http://icjr.or.id/mengatur-ulang-hukum-penyadapan-indonesia/

USA Today (2016, 23 Maret) *"A list of amicus briefs in support of Apple for the 22 March 2016"*. diakses dari http://www.usatoday.com/story/tech/news/2016/02/19/apple-fbi--court-march-22-riverside-march22/80635402/

70 percent-Sandvine, 2016 *Global Internet Phenomena Spotlight: Encrypted Internet Traffic* (Waterloo, ONT: Sandvine, 2016), https://www.sandvine.com/trends/encryption.html;

https://www.amnesty.org/en/who-we-are/
http://www.idsirtii.or.id/berita/baca/41/setahun-40-juta-konsumen-jadi-korban-hacking-.html
http://www.oecd.org/about/membersandpartners/

Peraturan

Amnesty International Policy on Encryption.

China Law Translate, "Counter-Terrorism Law (Initial Draft).

Communications Assistance for Law Enforcement Act (CALEA).

Data Protection Act 1998.

Electronic Communications and Information Society Services Law.

European Commision for Democracy Though Law, *"Federal Law of The Federal Security Service of The Russian Federation"*

Law No. 2004-575 of 21 June 2004 on Congfidence in Digital Economy.

Peraturan Pemerintah Nomor 19 Tahun 2000 tentang Tim Gabungan Pemberantasan Tindak Pidana Korupsi.

Peraturan Pemerintah Nomor 52 Tahun 2000 tentang Penyelenggaraan Telekomunikasi.

Perkapolri Nomor 5 Tahun 2010 tentang Tata Cara Penyadapan Pada Pusat Pemantauan Kepolisian Negara Republik Indonesia

Perkominfo Nomor 11 Tahun 2006 tentang Teknis Penyadapan Terhadap Informasi untuk Pertahanan dan Keamanan Negara.

Perkominfo Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi.

Regulation of Investigatory Powers Act 2000.

The Civil Rights Framework for The Internet.

The Electronic Communications and Transactions Act.

The Electronic Transactions and Cyber Security Act.

The Information Technology Act 2000.

The General Data Protection Regulation (GDPR).

The Law on Cryptography.

The Law on the Protection of Privacy in Electronic.

The OECD Guidelines for The Protection of Privacy and Transborder Flows of Personal Data.

Undang-Undang Dasar 1945

Undang-Undang Nomor 11 Tahun 2008 jo. Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang Nomor 5 Tahun 1997 tentang Psikotropika.

Undang-Undang Nomor 35 Tahun 2009 tentang Narkotika.

Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi.

Undang-Undang Nomor 31 Tahun 1999 jo. Undang-Undang Nomor 20 Tahun 2001 tentang Pemberantasan Tindak Pidana Korupsi.

Undang-Undang Nomor 30 Tahun 2002 tentang Komisi Pemberantasan Korupsi.

Undang-Undang Nomor 18 Tahun 2003 tentang Advokat.

Undang-Undang Nomor 21 Tahun 2007 tentang Tindak Pemberantasan Perdagangan Orang.

Undang-Undang Nomor 17 Tahun 2011 tentang Intelijen Negara.

Undang-Undang Nomor 18 Tahun 2011 tentang Perubahan Atas Undang-Undang Nomor 22 Tahun 2004 tentang Komisi Yudisial.

UN Guiding Principles on Business and Human Rights (UNGPs).