

**ANALISIS YURIDIS TINDAK PIDANA *CYBER CRIME*
PHISING DALAM KETENTUAN HUKUM POSITIF
INDONESIA**

***JURIDICAL ANALYSIS OF THE CRIMINAL OFFENSE OF
CYBER CRIME PHISING IN THE PROVISIONS OF
INDONESIAN POSITIVE LAW***



Oleh:

BERDIAWAN BENYAMIN

B011171585

**PROGRAM STUDI SARJANA ILMU HUKUM
FAKULTAS HUKUM UNIVERSITAS HASANUDDIN
MAKASSAR
2024**

HALAMAN JUDUL

**ANALISIS YURIDIS TINDAK PIDANA *CYBER CRIME*
PHISING DALAM KETENTUAN HUKUM POSITIF
INDONESIA**

Diajukan Sebagai Salah Satu Syarat Untuk Mencapai Gelar Sarjana
Pada Program Studi Sarjana Ilmu Hukum

Disusun dan diajukan oleh:

BERDIAWAN BENYAMIN

B011171585

**PROGRAM STUDI SARJANA ILMU HUKUM
FAKULTAS HUKUM UNIVERSITAS HASANUDDIN
MAKASSAR
2024**

PENGESAHAN SKRIPSI

**ANALISIS YURIDIS TINDAK PIDANA *CYBER CRIME PHISING* DALAM
KETENTUAN HUKUM POSITIF INDONESIA**

Disusun dan diajukan oleh :

BERDIAWAN BENYAMIN

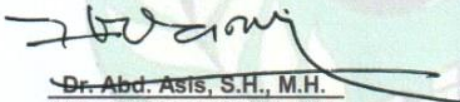
B011171585


Telah dipertahankan di hadapan Panitia Ujian Skripsi yang dibentuk dalam rangka Penyelesaian Studi Program Sarjana Departemen Hukum Pidana Program Studi Ilmu Hukum Fakultas Hukum Universitas Hasanuddin Pada hari Kamis, 14 Maret 2024 Dan dinyatakan telah memenuhi syarat kelulusan.

Menyetujui,

Pembimbing Utama

Pembimbing Pendamping


Dr. Abd. Asis, S.H., M.H.
NIP. 196206181989031002


Prof. Dr. Maskun, S.H., LL.M.
NIP. 197906092009121001

Ketua Program Studi Sarjana Ilmu Hukum




Dr. Muhammad Iham Arisaputra, S.H., M.Kn.
NIP. 198408182010121005

PERSETUJUAN PEMBIMBING

ANALISIS YURIDIS TINDAK PIDANA *CYBER CRIME* *PHISING* DALAM KETENTUAN HUKUM POSITIF INDONESIA

Diajukan dan disusun oleh:

Berdiawan Benyamin

B011171585

Untuk Tahap UJIAN SKRIPSI

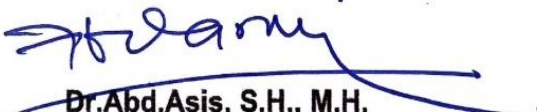
Pada Tanggal 14 Maret 2024


Menyetujui:

Komisi Penasehat

Pembimbing utama

pembimbing pendamping


Dr. Abd. Asis, S.H., M.H.
NIP. 196206181989031002


Prof. Dr. Maskun, S.H., LL.M.
NIP. 19761129 1999031005



KEMENTERIAN PENDIDIKAN, KEBUDAYAAN,
RISET, DAN TEKNOLOGI
UNIVERSITAS HASANUDDIN
FAKULTAS HUKUM

Jln. Perintis Kemerdekaan KM.10 Kota Makassar 90245, Propinsi Sulawesi Selatan
Telp : (0411) 587219,546686, Website: <https://lawfaculty.unhas.ac.id>

PERSETUJUAN MENEMPUH UJIAN SKRIPSI

Diterangkan bahwa skripsi mahasiswa :

Nama	: BERDIAWAN BENYAMIN
N I M	: B011171585
Program Studi	: Ilmu Hukum
Departemen	: Hukum Pidana
Judul Skripsi	: ANALISIS YURIDIS TINDAK PIDANA (CYBER CRIME PHISING) DALAM KETENTUAN HUKUM POSITIF INDONESIA

Memenuhi syarat untuk diajukan dalam ujian skripsi sebagai ujian akhir program studi.

Makassar, Maret 2024



Prof. Dr. Hamzah Halim, SH., M.H., M.A.P.
NIP: 19731231 199903 1 003

PERNYATAAN KEASLIAN

Nama : Berdiawan Benyamin
Nim : B011171585
Program Studi : Sarjana Ilmu Hukum

Menyatakan dengan ini bahwa Skripsi dengan judul **ANALISIS YURIDIS TINDAK PIDANA CYBER CRIME PHISING DALAM KETENTUAN HUKUM POSITIF INDONESIA** adalah benar-benar karya saya sendiri. Hal yang bukan merupakan karya saya dalam penulisan Skripsi ini diberi tanda *citasi* dan ditunjukkan dalam daftar pustaka.

Apabila dikemudian hari terbukti pernyataan saya tidak benar maka saya bersedia menerima sanksi sesuai peraturan Menteri Pendidikan Nasional Republik Indonesia Nomor 17 Tahun 2010 dan Peraturan Perundang-Undangan yang berlaku

Makassar, 14 Maret 2024

Yang menyatakan



Handwritten signature of Berdiawan Benyamin.

Berdiawan Benyamin

UCAPAN TERIMA KASIH

Shalom, assamualaikum Wr Wb, salam kebajikan, hidup Mahasiswa

Puji syukur saya panjatkan sebesar-besarnya kepada Tuhan Yesus Kristus atas berkah dan limpah-Nya sehingga penulis dapat menyelesaikan Skripsi dengan judul Analisis Yuridis Tindak Pidana *Cyber Crime Phising* Dalam Ketentuan Hukum Positif Indonesia sebagai persyaratan wajib bagi mahasiswa fakultas hukum universitas Hassanuddin guna memperoleh gelar sarjana hukum. Pada kesempatan ini pula penulis panjatkan dan hanturkan doa dan ucapan terima kasih yang sebesar-besarnya dan sedalam-dalamnya kepada ayahanda yang pada proses penyusunan skripsi ini berpulang kepada yang maha kuasa semoga amal ibadah almarhum brika Benyamin Pare diterima disisi Tuhan Yesus Kristus amin.

Dalam proses penyusunan skripsi ini penulis sudah berusaha semaksimal mungkin namun penulis menyadari bila penulis hanya manusia biasa yang tak lepas dari segala kesalahan dan ketidak sempurnaan maka dari itu penulis senantiasa menerima kritik serta masukan saran yang dapat menyempurnakan skripsi ini.

Dalam penyusunan skripsi ini pula terdapat beberapa pihak yang senantiasa mendukung dan memberi motivasi kepada penulis dalam mengerjakan skripsi ini dan pada kesempatan ini penulis ingin berterima kasih kepada kedua orang tua ayahanda alm brika Benyamin Pare dan juga ibunda terkasih dan tercinta Ludia Tandi Kala. tak lepas pula dari

keluarga penulis kedua kakak penulis Lesmin Apriliani Tangaran dan Reny Tangaran dan juga kedua keponakan penulis yang selalu menghibur penulis dalam mengerjakan skripsi Levin dan Livia. Adapula beberapa pihak yang membantu dan memberi masukan kepada penulis dalam penyusunan skripsi ini, yakni kepada :

1. Bapak Prof. Dr. Ir. Jamaluddin Jompa, M.Sc. selaku Rektor Universitas Hasanuddin beserta jajarannya
2. Bapak Prof. Dr. Hamzah Halim, S.H., M.H., MAP. Selaku Dekan Fakultas Hukum Universitas Hasanuddin beserta jajarannya
3. Bapak Dr. Abd. Asis, S.H., M.H. sebagai pembimbing utama penulis yang membantu memberi masukan dan saran guna penyempurnaan dalam penulisan skripsi penulis.
4. Bapak Prof. Dr. Maskun, S.H.,LL.M. sebagai pembimbing pendamping yang telah memberikan masukan serta saran guna penyempurnaan dalam penulisan skripsi penulis.
5. Bapak Prof. Dr. Andi Muhammad Sofyan, S.H., M.H. sebagai penguji I penulis dalam memberikan masukan dan saran bagi penulis guna penyempurnaan penulisan skripsi penulis.
6. Bapak Andi muhammad Aswin Anas S.H., M.H. sebagai penguji II penulis dalam memberikan masukan dan saran bagi penulis guna penyempurnaan penulisan skripsi penulis.

7. Ibu Eka Merdekawati Djafar, S.H., M.H. sebagai pembimbing akademik yang sudah memberikan masukan dan saran untuk penulis selama menjalani perkuliahan.
8. Seluruh dosen Fakultas Hukum Universitas Haasanuddin serta seluruh Staff/Pegawai Fakultas Hukum Universitas Hasanuddin yang turut membantu penulis selama menjalani aktifitas di kampus, baik yang bersifat akademik maupun non akademik.
9. Terima kasih kepada sahabat penulis Olaf, yeni, edwin, diana.c, dan erik, diana.n, santi dan opi yang selalu setia menemani penulis dalam susah maupun senang.
10. Terima kasih sebanyak-banyaknya kepada pujaan hati Leony Christina Angel Palallo yang setia menemani, memberi semangat, motivasi, bantuan secara materil dan immateril serta doa yang tulus buat penulis.
11. Terima kasih kepada seluruh teman-teman ADAKAH ? harcan, wisdar, diaulhaq, agung, tammam dan akhsan. yang sudah setia menjadi teman penulis dari mahasiswa baru hingga menjadi mahasiswa seperti sekarang.
12. Terima kasih kepada kakanda, teman-teman dan dinda kak tiku, michael, tika, grace.s, grace.a, wasti, mama, ricky, edo.c, tavo, jovi, vero, christo, melki, iren, kevin, meldrix, rei edo.j, vivi, tirza, yuyum, diky, gladys, satria, indah, mei, dan seluruh pihak yang tidak penulis sebutkan satu persatu.

13. Terima kasih kepada seluruh teman angkatan 2017 PLEDOI yang sudah menemani penulis dalam perkuliahan selama di UNHAS.
14. Terima kasih kepada seluruh teman KKN KALTIM-KALSEL yang sudah senantiasa membantu dan memberi dukungan kepada penulis.
15. Terima kasih kepada dewan perwakilan mahasiswa fakultas hukum periode 2019-2020 yang telah menjalani kepengurusan bersama penulis.
16. Terima kasih kepada keluarga besar Ukm Bola Basket Hukum yang menemani kepengurusan bersama penulis.
17. Terima kasih kepada keluarga Ukm Sepak Bola hukum unhas yang menemani kepengurusan bersama penulis.
18. Terima kasih kepada keluarga Ukm LKMP dalam kepengurusan bersama penulis.
19. Terima kasih kepada persekutuan mahasiswa kristen FH-UH selama menjalani kepengurusan bersama dengan penulis.
20. Terima kasih kepada GMKI yang telah menjalani kepengurusan bersama dengan penulis.
21. Terima kasih kepada teman-teman kelas mata kuliah umum dalam menemani penulis selama perkuliahan.
22. Terima kasih kepada seluruh pihak yang terlibat dalam membantu penulis menyusun skripsi ini yang tidak dapat penulis tuliskan satu persatu.

Akhir kata semoga skripsi ini dapat bermanfaat bagi masyarakat dan negara, semoga Tuhan Yesus Kristus senantiasa menilai perbuatan dan amal kita sebagai ibadah dan ucapan syukur kepada sang pencipta Amin.

Makassar, 14 Maret 2024

Yang menyatakan

A handwritten signature in black ink, appearing to read 'Berdiawan Benyamin', written in a cursive style.

Berdiawan Benyamin

ABSTRAK

BERDIAWAN BENYAMIN (B011171585), dengan judul “*Analisis Yuridis Tindak Pidana Cyber Crime Phising Dalam Ketentuan Hukum Positif Indonesia*”. Dibawah bimbingan **Abd. Asis** sebagai pembimbing utama dan **Maskun** sebagai pembimbing pendamping.

Penelitian ini bertujuan untuk mengetahui pengaturan hukum tentang *cyber crime phising* dalam ketentuan hukum positif indonesia serta untuk menentukan apakah asas referensi hukum dalam undang-undang republik indonesia nomor 19 tahun 2016 tentang informasi dan transaksi elektronik dan undang-undang nomor 27 tahun 2022 tentang perlindungan data pribadi.

Penelitian ini menggunakan metode penelitian normatif dengan menjadikan undang-undang republik indonesia nomor 19 tahun 2016 tentang informasi dan transaksi elektronik dan undang-undang republik indonesia nomor 27 tahun 2022 tentang perlindungan data pribadi sebagai sumber hukum utamanya. Dan studi kepustakaan (*library research*) yaitu penelitian yang dilakukan dengan memperoleh data sekunder berkaitan dengan penelitian skripsi ini.

Penelitian ini menyimpulkan bahwa :(1) tindak pidana *cyber crime phising* diatur pada pasal 32 ayat 1 undang-undang republik indonesia nomor 19 tahun 2016 bila mana terjadi perubahan pada objek data pribadi dan pada pasal 65 ayat 1 undang-undang republik indonesia nomor 27 tahun 2022 mengatur mengenai *cyber crime phising* dalam hal spesifikasi data yang bersifat umum dan data bersifat spesifik. (2) menurut asas preferensi hukum maka tindak pidana *cyber crime phising* yang diatur dalam undang-undang republik indonesia nomor 19 tahun 2016 pasal 32 ayat 1 dikesampingkan atau berlaku undang-undang republik indonesia nomor 27 tahun 2022 pasal 65 ayat 1.

Kata kunci: *cyber crime phising*. Kejahatan *cyber*. perlindungan data pribadi.

ABSTRACT

BERDIAWAN BENYAMIN (B011171585), with the title "**Juridical Analysis of Cyber Crime Phishing in Indonesian Positive Law Provisions**". Under the guidance of Abd. Asis as the main supervisor and Maskun as the co-supervisor.

This study aims to determine the legal regulation of cyber crime phishing in the provisions of Indonesian positive law and to determine whether the principle of legal reference in the law of the republic of Indonesia number 19 of 2016 concerning electronic information and transactions and law number 27 of 2022 concerning personal data protection.

This research uses normative research methods by making the law of the republic of indonesia number 19 of 2016 concerning information and electronic transactions and the law of the republic of indonesia number 27 of 2022 concerning personal data protection as the main legal source. And library research, which is research conducted by obtaining secondary data related to this thesis research.

This research concludes that: (1) the criminal offense of cyber crime phishing is regulated in article 32 paragraph 1 of the law of the republic of indonesia number 19 of 2016 when there is a change in the object of personal data and in article 65 paragraph 1 of the law of the republic of indonesia number 27 of 2022 regulates cyber crime phishing in terms of general data specifications and specific data. (2) According to the principle of legal preference, the criminal offense of cyber crime phishing regulated in Law of the Republic of Indonesia Number 19 of 2016 Article 32 Paragraph 1 is ruled out or applies Law of the Republic of Indonesia Number 27 of 2022 Article 65 Paragraph 1.

Keywords: cyber crime phishing. Cyber crime. personal data protection.

DAFTAR ISI

	Halaman
HALAMAN JUDUL	i
PENGESAHAN SKRIPSI	ii
PERSETUJUAN PEMBIMBING	ii
PERSETUJUAN MENEMPUH UJIAN SKRIPSI.....	iv
PERNYATAAN KEASLIAN	v
UCAPAK TERIMA KASIH	vi
ABSTRAK.....	xi
ABSTRACT.....	xii
DAFTAR ISI	xiii
BAB I PENDAHULUAN	1
A. Latar belakang	1
B. Rumusan masalah	9
C. Tujuan penelitian	9
D. Kegunaan penelitian	10
1. Manfaat teoritis	10
2. Manfaat praktis	10
E. Keaslian penelitian.....	11
BAB II TINJAUAN PUSTAKA.....	15
A. Tinjauan Umum Tindak Pidana kejahatan internet	15
1. Penertian tindak pidana	15
2. Unsur-unsur tindak pidana.....	16
3. Cyber space	21
4. Cyber crime	23
5. Jenis-jenis cyber crime	27
B. Tinjauan umum mengenai phising	38
1. Pengertian phising.....	38
2. Jenis-jenis phising	41

C.	Pemahaman undang-undang republik indonesia- nomor 19 tahun 2016 tentang informasi dan transaksi elektronik	47
1.	Pengertian informasi elektronik dan transaksi elektronik	47
2.	Klasifikasi tindak pidana phising menurut uuri ite.....	48
D.	Pemahaman undang-undang republik indonesia- Nomor 27 tahun 2022 tentang perlindungan- Data pribadi	50
1.	Pengertian data pribadi dan Perlindungan data pribadi	50
2.	Asas dan penjelasan	50
3.	Klasifikasi tindak pidana phising Menurut uuri pdp 2022.....	52
E.	Tinjauan umum yurisdiksi dalam tindak pidana- Phising.....	53
1.	Penngertian yurisdiksi.....	53
2.	Prinsip-prinsip yurisdiksi secara umum	56
F.	Tinjauan umum mengenai asas	63
1.	Pengertian asas	63
G.	Tinjauan umum mengenai norma.....	65
1.	Pengertian dan jenis-jenis norma.....	65
H.	Tinjauan umum mengenai jenis-jenis ilmu- Dan metode penafsiran hukum	70
1.	Jenis-jenis ilmu penafsiran.....	70
2.	Jenis-jenis metode penafsiran	75
I.	Tinjauan umum mengenai asas preferensi hukum.....	79
BAB III METODE PENELITIAN.....		81
A.	Tipe dan Pendekatan penelitian.....	81

B.	Jenis dan sumber bahan hukum	84
C.	Analisis bahan hukum	84
BAB IV PEMBAHASAN		86
A.	KLASIFIKASI TINDAK PIDANA CYBER CRIME- PHISING DALAM KETENTUAN HUKUM POSITIF- INDONESIA	86
1.	klasifikasi tindak pidana cyber crime phising- dalam undang-undang republik indonesia- nomor 19 tahun 2016 tentang perubahan- informasi dan transaksi elektronik	89
2.	klasifikasi tindak pidana cyber crime phising- dalam undang-undang nomor 27 tahun 2022- tentang perlindungan data pribadi	94
3.	perluasan pemahaman tindak pidana phising	98
4.	pertentangan norma undang-undang- ITE 2016 dan undang-undang PDP 2022- Dalam tindak pidana phising	103
B.	penentuan asas preferensi hukum dalam- tindak pidana cyber crime phising berdasarkan- ketentuan hukum positif indonesia	116
BAB V PENUTUP		128
A.	KESIMPLAN	128
B.	SARAN	129
DAFTAR PUSTAKA		131

BAB I

PENDAHULUAN

A. Latar Belakang

Sejarah perkembangan komputer dan internet tak dapat dipisahkan, karena internet sendiri membutuhkan perangkat komputer untuk mengaksesnya dan seiring perkembangannya internet sudah tidak hanya dapat diakses melalui komputer saja, terdapat beberapa perangkat seperti *smartphone*, televisi dan berbagai alat teknologi lainnya. Berkembangnya internet membuat globalisasi sangat cepat, faktor kecepatan internet membuat jarak sangat semu. Informasi yang didapat bisa sangat aktual atau dengan kata lain tidak dibatasi oleh jarak, bahkan dibandingkan dengan beberapa perkembangan media komunikasi seperti radio dan televisi, internet sangat cepat mengglobalisasi, hal ini didasarkan oleh data, bahwa untuk menjangkau pengguna sebanyak 60 juta manusia, radio membutuhkan waktu setidaknya 30 tahun dan untuk televisi membutuhkan waktu 15 tahun dan untuk internet sendiri hanya membutuhkan waktu 3 tahun.¹

Terdapat beberapa faktor yang membedakan internet dari alat media lainnya sebagai contoh internet mempunyai fungsi yang sangat luas yang tentunya dipengaruhi oleh perkembangan zaman dan tuntutan akan pemenuhan kebutuhan manusia yang selalu ingin serba

¹ Rusito, 2021, Teknologi internet, dasar internet, *internet of things* (IOT) dan bahasa

cepat dan tidak dibatasi oleh jarak. Sifat internet yang sangat luas memungkinkan juga beberapa sektor memanfaatkannya seperti sektor perbankan, Kesehatan, pertanian, jasa dan barang, ritel, transportasi, komunikasi, dan perusahaan yang bergerak di sektor lain nya.

Internet berubah menjadi sebuah kebutuhan pokok sejalan dengan data yang dikemukakan oleh *Cisco Annual Internet Report 2018-2023*, menunjukkan bahwa hampir dua pertiga populasi global akan memiliki akses internet pada tahun 2023 dan akan ada 5,3 miliar total pengguna internet atau 66 persen populasi global dan pada tahun 2023 angka ini naik dari 3,9 miliar persen populasi global pada tahun 2018.² Hal ini sejalan dengan data yang dikemukakan oleh Asosiasi Penyelenggara Jasa Internet Indonesia yang menunjukkan bahwa pada tahun 2018 pengguna internet nasional sebesar 171,17 juta jiwa atau sekitar 64,8 persen dari seluruh Warga Negara Indonesia dan jika menurut Badan Pusat Statistik Indonesia, populasi Indonesia tahun 2019 berjumlah 266,911,900 juta jiwa dan pengguna internet tahun 2019 diperkirakan sebanyak 196,7 juta pengguna internet.³

Angka ini naik lagi saat terjadinya pandemi *Corona Virus Disease 2019* selanjutnya disebut *covid-19* di mana internet menjadi sangat penting, karena banyak kegiatan yang di lakukan secara

² Cisco, *White paper Cisco annual internet report (2018-2023), global forecast/analysis that assesses digital transformation across various business segments (enterprise, small-to-medium business, public sector, and service provider)*.(tanpa halaman).

³ Profil Internet Indonesia 2022, Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), Juni 2022.(tanpa halaman).

daring. Badan Pusat Statistik selanjutnya disebut BPS dari survei Statistik Telekomunikasi Indonesia menyebutkan bahwa pengguna internet dalam rumah tangga mencapai 82,07 persen pada tahun 2021 angka ini naik dari tahun 2017-2021 yang mencapai persentase 65,87 persen.⁴ Membandingkan dari dua data yang dikemukakan oleh Asosiasi Penyelenggara Jasa Internet Indonesia yang menyatakan bahwa sekitar 210 juta pengguna internet pertahun 2022 dan dari badan pusat statistika menunjukkan bahwa penduduk Indonesia pada tahun 2022 sebanyak 275,77 juta jiwa dari survei yang dilakukan di atas menunjukkan persentase sebesar 76,11 persen angka ini naik dari tahun sebelumnya. Hal ini membuat peran internet sangat penting bagi kepentingan masyarakat umum.

Berdasarkan data yang telah dikemukakan, terdapat beberapa pertimbangan seperti sifat dari internet, tuntutan pemenuhan akan internet, kemudahan mengakses internet serta jangkauannya yang sangat luas memunculkan kerentanan terhadap masalah keamanan. Pengguna yang sangat banyak juga menjadi faktor penting internet mengglobalisasi sangat cepat. Hal ini diperparah lagi dengan kurangnya pengetahuan akan internet, membuat internet sangat rentan terhadap serangan *cyber* atau yang biasa di kenal dengan istilah *cyber crime*.

⁴ Tri Sutarsih, dkk, 2022, Statistik Telekomunikasi Indonesia 2021, Badan Pusat Statistik, Jakarta, hlm. 20.

Terdapat beberapa istilah di dalam kejahatan *cyber* yang para pakar hukum gunakan antara lain *computer misuse*, *computer abuse*, *computer fraud*, *computer-related crime*, *computer-assisted crime*, *computer crime* atau kejahatan mayantara dan berbagai istilah lainnya. Namun penulis lebih sepekat terhadap penyebutan *cyber crime* yang selanjutnya akan penulis gunakan selama penulisan skripsi ini.

Cyber crime dalam abad ini berkembang sangat pesat terdapat beberapa kejahatan *cyber* yang memakai modus operandi *hacker*, *phising* dan beberapa modus operandi lainnya. Berbeda dengan *hacker*, *phising* bekerja dengan memanfaatkan psikologis dari sang korban tanpa langsung meretas sistem. Jadi dalam hal modus operandi *phising* kelengahan dari korbanlah yang dimanfaatkan para *phisher/ phiser* sebutan bagi pelaku *phising* (yang selanjutnya demi konsistensi penulisan akan di gunakan kata *phiser*). Istilah *phising* sendiri dikenalkan oleh *Newsgroup Usenet Online Service America Online* selanjutnya disebut AOL pada 2 Januari tahun 1996 yang adalah salah satu penyedia akses internet dengan jutaan orang *login* ke layanan ini setiap hari. Ketika *account* AOL dicuri oleh *hacker* (yang sekarang dikenal dengan *phiser*) dengan melakukan *scamming password* dari *user-user* AOL yang tidak dikenal.⁵

Kasus *phising* sudah lama sekali terjadi bahkan pada awal kemunculannya korbanlah yang menjadi pihak disalahkan karena

⁵ Cahaya Wahyu, "Phising dan cara menghindarinya", cahayawahyu.wordpress.com, 2013, (opini).

kelalaiannya sendiri yang memberikan data pribadinya kepada orang lain. Akan tetapi dewasa ini *phising* sudah sangat berkembang dikarenakan pemanfaatan teknologi yang sangat canggih membuat kejahatan ini sangat susah sekali ditindak. Pada kasus perusahaan manufaktur *spare parts* luar angkasa bernama *Fischer Advanced Composite Components* selanjutnya disebut FAAC yang menjadi langganan *Boeing* dan *Airbus* juga tak luput menjadi korban *phising*, peretas menyamar sebagai *-Chief Executive Officer* selanjutnya disebut (CEO)- CEO FAAC dan mengirimkan *e-mail* tersebut kepada *staff accounting*. Peretas yang menyamar sebagai CEO gadungan meminta dana sebesar 47 juta dolar untuk dikirimkan ke akun peretas dengan dalih untuk proyek akuisi kasus ini dikenal dengan *fake president incident*.⁶

Indonesia sendiri ada kasus yang pernah terkuak menargetkan warga negara Amerika Serikat yang menggunakan modus operandi *phising*, kasus yang pelaku berinisial SFR dan MCL. pelaku memanfaatkan bantuan bagi para korban terdampak *Covid-19* yang di tujukan kepada warga negara Amerika Serikat. MCL membuat laman situs *website* yang sangat mirip dengan laman situs *website* resmi dari Pemerintah Amerika Serikat. Lalu tersangka SFR menyebarkan alamat *website* tersebut dengan menggunakan layanan *SMS blast* kepada 20 juta warga negara amerika serikat secara masal.

⁶ 5 kasus phising paling mengguncang dunia, asia quest indonesia, 18 oktober 2022, aqi.co.id. (koran online).

Dari tautan SMS yang terkirim 30.000 warga amerika percaya dan mengklik tautan yang ada. Berdasarkan hal ini tersangka MCL dan SFR menggunakan data yang sudah diambil dari *website* mereka, untuk digunakan mengambil dana batuan yang ada di *website* resmi milik pemerintah amerika.⁷

Sejalan dengan laporan yang dikemukakan oleh badan siber dan sandi negara selanjutnya disebut BSSN menyebutkan ada 164.131 kasus email phising di Indonesia pada 2022 terbagi 3 kategori email phising pribadi menyumbang kasus terbanyak dengan 59.210 kasus, kasus phising yang berasal dari email group sebanyak 52.744 kasus dan kasus email phising lainnya sebanyak 52.177 kasus.⁸ Kasus phising di Indonesia juga dilaporkan direktorat tindak pidana siber bareskrim polri menunjukkan ada 5.579 serangan phising yang terjadi di Indonesia selama kuartal kedua 2022 yang mengincar beberapa sektor yaitu Lembaga keuangan dengan presentase sebanyak 41%, *E-commerce* sebanyak 32%, media sosial sebanyak 21%, game online dan aset kripto dengan presentase sebanyak 6%.⁹ Adapun Lembaga Indonesia *anti-phising exchange* selanjutnya disebut IDADX melaporkan pula kejahatan phising yang terjadi di Indonesia pada kuartal 3-2023 sebanyak 9.823 kasus yang terjadi pada bulan juli

⁷ Farid, dua WNI bikin situs palsu, raup dana covid AS US\$60 juta, 16 April 2023, www.cnnindonesia.com. (koran online).

⁸ Dimas bayu, ada 164.131 kasus email phising di Indonesia pada tahun 2022, 28 maret 2023, www.dataindonesia.id (koran online)

⁹ Annissa mutia, ada 5 ribu serangan phising terjadi di RI pada kuartal 2-2022 ini lembaga paling banyak di incar, 23 agustus 2022, www.dataindonesia.id. (koran online).

sampai dengan September. Pada laporan kuartal ketiga ini sektor media sosial memiliki presentase yang lebih tinggi diantara sektor lainnya sebanyak 55,45%, Lembaga keuangan 22,7%, *E-commerce* dan ritel sebanyak 17,69%, ISP persentase 4,03%, game 0,27%, perjudian 0,18%, instansi pemerintah sebanyak 0,09%. Walaupun angka ini menunjukkan penurunan dari kuartal 2-2023 dari angka 20.330 tetapi Indonesia tetap menjadi posisi pertama sebagai negara yang menghosting situs phishing domain .id selama kuartal 3 tahun 2023.¹⁰

Melihat beberapa kasus di atas *cyber crime* merupakan suatu kejahatan yang sangat serius dan perlu adanya payung hukum untuk melindungi warga negara Indonesia. Dalam dunia internasional terdapat *convention of cyber crime Eruopean Treaty Series* yang mengatur tentang *cyber crime*. Di Indonesia sendiri terdapat Undang-undang Republik Indonesia selanjutnya disebut UURI Nomor 11 Tahun 2008 Tentang Informasi Transaksi Elektronik yang telah diperbaharui menjadi UURI Nomor 19 Tahun 2016 selanjutnya disebut UURI ITE 2016. Selain itu terdapat pula UURI Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi selanjutnya disebut UURI PDP 2022. Pembuatan UURI PDP 2022 dinilai terlambat karena telah dicanangkan pada tahun 2021 sebelum terjadi kasus kebocoran data

¹⁰ Indonesia *Anti-phishing data exchange* (IDADX), laporan aktivitas phishing domain, oktober 2023, hlm. 2-6.

penduduk Indonesia dan baru disepakati pada 17 oktober 2022 setelah terjadinya kebocoran data penduduk Indonesia.

pengesahan UURI PDP 2022 menjadi angin segar bagi masyarakat Indonesia dikarenakan adanya suatu perlindungan hukum bagi masyarakat Indonesia dalam menjamin kebebasan data pribadi yang menjadi suatu hak konstitusional warga negara. Dibalik terdapatnya jaminan hukum bagi warga negara muncul pula suatu norma hukum yang baru yang telah dibawa oleh UURI PDP, norma baru ini tentu saja memerlukan suatu jalinan dan keselarasan agar tidak munculnya pertentangan dan multipersepsi atas suatu norma hukum yang berlaku di Indonesia. Pada UURI ITE dan UURI PDP mengatur data pribadi baik dalam perlindungan hak data pribadi dan jaminan hukumnya. Maka dari itu pula muncul perbedaan pandangan dan persepsi dari kedua undang-undang ini. Maka diperlukan penafsiran hukum yang mendalam mengenai klasifikasi atau pun definisi yang diberikan kedua undang-undang ini. Terdapat berbagai risiko munculnya konflik interpretasi antara dua undang-undang atau ketentuan yang berbeda yang akan membuat penegak hukum mungkin kesulitan dalam menentukan undang-undang yang mana yang harus diterapkan dalam situasi tertentu.

Berdasarkan latar belakang yang penulis paparkan di atas, sangat menarik perhatian penulis untuk mengetahui dan membahas lebih dalam lagi. bagaimana pengaturan *cyber crime* dalam hal ini

terkhususnya *phising* dalam hukum positif Indonesia dan konstruksi norma yang dibangun, maka dari itu penulis menarik judul penelitian ini adalah “**Analisis Yuridis Tindak Pidana *Cyber Crime Phising* Dalam Ketentuan Hukum positif Indonesia**” sebagai studi hukum.

B. Rumusan Masalah

Berdasarkan uraian latar belakang di atas, maka penulis menarik rumusan masalah sebagai berikut:

1. Bagaimanakah klasifikasi tindak pidana *Cyber Crime Phising* dalam ketentuan hukum positif Indonesia?
2. Apakah penentuan asas preferensi hukum dalam tindak pidana *cyber crime phising* berdasarkan ketentuan hukum positif Indonesia?

C. Tujuan Penelitian

Berdasarkan rumusan masalah di atas, maka tujuan penelitian ini adalah sebagai berikut:

1. Untuk mengetahui bagaimanakah pengaturan tindak pidana *Cyber Crime Phising* dalam ketentuan hukum positif Indonesia.
2. Untuk mengetahui apakah penentuan asas preferensi hukum dalam tindak pidana *cyber crime phising* berdasarkan hukum positif Indonesia .

D. Kegunaan Penelitian

Adapun kegunaan yang diharapkan dari penelitian ini adalah sebagai berikut:

1. Manfaat teoretis
 - a. Penelitian ini diharapkan dapat memberikan sumbangan pemikiran bagi kemajuan ilmu pengetahuan bagi masyarakat indoneisa maupun internasional khususnya dibidang hukum pidana.
 - b. Diharapkan memberi tambahan pengetahuan bagi aparat penegak hukum dan pembuat undang undang betapa pentingnya masalah keamanan dari tindak kejahatan *cyber crime phising*.
2. Manfaat praktis
 - a. Diharapkan dapat digunakan sebagai acuan dalam mengembangkan pemikiran logis yang tersistematis dan menjadi tolak ukur kemampuan penulis dalam mengimplementasikan pengetahuan yang selama ini didapatkan.
 - b. Hasil penulisan ilmiah ini dapat membantu perkembangan hukum di indonesia dalam pembentukan regulasi hukum *cyber crime* dan dalam hal penegakan hukum *cyber crime* di Indonesia.

E. Keaslian Penelitian

Dari hasil pencarian penelitian untuk menjamin perbandingan, ditemukan hasil penelitian terdahulu yang mempunyai kemiripan seperti berikut:

Nama Penulis	:	Hilman Rusidi
Judul Tulisan	:	Petanggungjawaban Pidana Terhadap Pelaku Tindak Pidana <i>Cybe Crime Phising</i> (Studi Kasus Putusan Pengadilan Negeri Medan Nomor :3006/Pid.Sus/2017/PN.Mdn.
Kategori	:	Skripsi
Tahun	:	2019
Perguruan Tinggi	:	Univesitas Sriwijaya Palembang
Uraian		Rencana Penelitian
Isu dan Permasalahan	:	<p>Penelitian Terdahulu</p> <p>Bertujuan mengetahui bagaimana pertanggung jawaban <i>cyber crime phising</i> dengan metode atau teknik phising yang dilakukan oleh pelaku berdasarkan putusan nomor 3006/Pid.Sus/2017/PN.Mdn.</p> <p>Penulis bertujuan mengetahui bagaimana batasan dan pengaturan terhadap uuri ite dan uuri pdp dan bagaimana konflik norma yang terjadi antar kedua undang-undang dan Bagaimana penyelesaian</p>

			konflik antar norma.
Metode Penelitian	:	Normatif	Normatif
Hasil dan Pembahasan	:	Berdasarkan hasil penelitian dari skripsi ini diketahui bahwa pertanggungjawaban pidana terhadap pelaku tindak pidana <i>cybe crime phishing</i> telah dicantumkan dalam undang-undang nomor 11 tahun 2008 tentang informasi dan transaksi elektronik pasal 32 ayat 2 dan pasal 35	Hasil penelitian penulis menunjukkan bahwa ketentuan <i>cyber crime phishing</i> diatur dalam uuri ite dan uuri pdp dan bagaimana penyelesaian konflik norma antar uuri ite dan uuri pdp.
Nama Penulis	:	M. Bahrun Ardiansyah	
Judul Tulisan	:	Analisis Hukum Tentang Perilaku Tindak Pidana <i>Cyber Crime</i> Yang Berupa Phising	
Kategori	:	Skripsi	
Tahun	:	2022	
Perguruan Tinggi	:	Fakultas Hukum Univesitas Muhammadiyah Palembang	
Uraian		Penelitian Terdahulu	Hasil Penelitian
Isu dan Permasalahan	:	Adanya kendala atas perlindungan data pribadi kurangnya pengaturan	Konflik norma yang terjadi antara uuri ite dan uuri pdp

		dalam uu ite untuk menjangkau akan klasifikasi data yang dilindungi sebagai bentuk memberikan kejelasan akan data yang dapat diakses.	membuat perlu adanya analisis yang tajam atas pemberlakuan dan batasan apa yang diatur dalam uuri ite dan uuri pdp mengenai penerapannya atas tindak pidana <i>cyber crime phishing</i> .
Metode Penelitian	:	Normatif	Normatif
Hasil dan Pembahasan	:	Hasil penelitian ini menunjukkan bahwa data pribadi yang bersifat elektronik termasuk dalam informasi elektronik yang dilindungi. Uuri ite mengenal sistem keamanan yang memberikan perlindungan terhadap data atau informasi terhadap akses illegal dengan adanya kode	Hasil penelitian menunjukkan bahwa klasifikasi <i>cyber crime phishing</i> yang diatur dalam uuri ite diatur pula dalam uuri pdp. Penelitian ini menggunakan asas preferensi hukum untuk menjadi

	akses atau password serta adanya gangguan data yang juga dikenal dalam uuri ite.	acuan dalam menangani konflik norma yang terjadi.
--	--	---

BAB II

TINJAUAN PUSTAKA

A. Tinjauan Umum Tindak Pidana Kejahatan Internet

1. Pengertian Tindak Pidana

Mengenai istilah dari tindak pidana, ahli hukum dan undang-undang di Indonesia memakai istilah nya masing-masing, bahkan dalam perundang–undangan tidak ditemukan definisi dari tindak pidana itu sendiri. Perbuatan pidana, peristiwa pidana, tindak pidana, delik dan lain sebagainya adalah istilah-istilah yang digunakan di indoneisa secara umum. Pemberlakuan hukum pidana di indoneisa berdasarkan asas konkordansi dapat diartikan bahwa sistem hukum pidana Indonesia mengadopsi hukum dari belanda, maka istilah tindak pidana berasal dari kata “*strafbaar feit*”, melahirkan istilah yang secara umum disebut perbuatan yang dapat atau boleh dihukum.¹¹

Ada beberapa pengertian dari para ahli hukum yang dapat penulis kutip antara lain:

- a. Menurut pendapat Moeljatno yang menjelaskan perbuatan pidana hanya merujuk kepada sifat perbuatan saja yaitu sifat yang dilarang dengan ancaman pidana kalau dilanggar, dan tindak pidana hanya memuat tiga hal yaitu subjek delik yang maksud oleh norma hukum (*norm addressaat*), perbuatan yang dilarang (*strafbaar*) dan ancaman pidana (*strafmaat*).¹²
- b. Menurut Van Hammel tindak pidana adalah *Eene wettelijke*

¹¹ Fitri Wahyuni, 2017, Dasar-dasar Hukum Pidana di Indonesia, PT Nusantara Persada Utama, Tangerang Selatan, hlm. 35.

¹² Lukman Hakim, 2020, Asas-Asas Hukum Pidana Buku Ajar Bagi Mahasiswa, Deepublish, Yogyakarta, hlm. 21.

omschreven menschelijke gedraging, onrechtmatig, strafwaardig e naan schuld te wijten (kelakuan manusia yang dirumuskan dalam undang-undang melawan hukum, yang patut dipidana dan dilakukan dengan kesalahan).¹³

- c. Profesor Van Hattum berpendapat bahwa sesuatu tindakan itu tidak dapat dipisahkan dari orang yang telah melakukan tindakan tersebut. Menurutnya perkataan *strafbaar* itu berarti *voor straf in aanmerking komend* atau *straf verdienen* yang juga mempunyai arti sebagai pantas dihukum, sehingga perkataan *strafbaar feit* yang digunakan oleh pembentuk undang-undang di dalam kitab undang-undang hukum pidana itu secara eliptis haruslah diartikan sebagai suatu tindakan karena telah melakukan tindakan semacam itu membuat orang menjadi dapat di hukum.¹⁴

2. Unsur-unsur Tindak Pidana

Pembahasan mengenai usaha untuk menjabarkan sesuatu rumusan delik ke dalam unsur-unsurnya maka dapat penulis mulai dengan sesuatu yang disebut sebagai “tindakan manusia”, dengan tindakan seseorang dapat melakukan sesuatu yang dilarang oleh undang-undang. Secara umum ilmu pengetahuan hukum pidana, “sesuatu tindakan” itu dapat merupakan *een doen* atau dapat merupakan “hal melakukan sesuatu” ataupun “hal tidak melakukan sesuatu”, yang kedua di dalam doktrin sering disebut *een nalaten* yang berarti “hal mengalpakkan sesuatu yang diwajibkan oleh undang-undang.”¹⁵

Beberapa pakar ahli pidana telah mencoba mendefinisikan

¹³ Moh. Mujibur Rohman, dkk, 2023, Asas-Asas Hukum Pidana, PT Global Eksekutif Teknologi, Padang, hlm. 4.

¹⁴ P.A.F.Lamintang, Franciscus Theojunior Lamintang. 2019. Dasar-dasar Hukum Pidana di Indonesia. Sinar Grafika. Jakarta. hlm. 182.

¹⁵ *Ibid.*, hlm. 191.

pengertian dari unsur-unsur tindak pidana, penulis mengutip pendapat yang dikemukakan oleh D. Schaffmeister bahwa:

tidak dapat dijatuhkan pidana karena suatu perbuatan yang tidak termasuk delik. Ini tidak berarti bahwa selalu dapat dijatuhkan pidana kalau perbuatan itu tercantum dalam rumusan delik.

Untuk itu diperlukan dua syarat: perbuatan itu bersifat melawan hukum dan dapat dicela.¹⁶

a. Aliran monisme

Unsur-unsur pidana yang dikemukakan aliran monisme yakni aliran pemikiran klasik oleh Simons, yang berpendapat bahwa aliran monisme unsur-unsur peristiwa pidana merupakan syarat seseorang untuk dipidana. Jadi apabila seseorang yang melakukan tindak pidana dan hendak dijatuhi pidana harus dipenuhi semua unsur-unsur dari tindak pidana dan jika salah satu unsur tidak ada maka tidak boleh dipidana. Unsur delik menurut aliran monisme adalah sebagai berikut:¹⁷

- 1) Perbuatan mencocoki rumusan delik;
- 2) Ada sifat melawan hukum (tidak ada alasan pembenar);
- 3) Ada kesalahan (tidak ada alasan pemaaf).

Dapat diartikan aliran monisme adalah aliran yang menggabungkan unsur objektif (perbuatan pidana) dan unsur subjektif (pertanggungjawaban pidana) menjadi satu bagian yang

¹⁶ D. Schaffmeister, N. Keijzer dan E.P.H. Sutoris terjemahan J.E. Sahetapy, 1995, Hukum Pidana, Liberty, Yogyakarta, hlm. 27.

¹⁷ Extrix Mangkeprijanto, 2019, Hukum Pidana Dan Kriminologi, Guepedia Publisher, hlm. 68-69.

utuh.

Alasan dari simons mengapa *strafbaar feit* itu harus dirumuskan seperti di atas adalah karena :

- 1) Untuk adanya suatu *strafbaar feit itu* disyaratkan bahwa di situ harus terdapat suatu tindakan yang dilarang ataupun yang diwajibkan oleh undang-undang, di mana pelanggaran kepada larangan atau kewajiban semacam itu sudah dinyatakan sebagai bagian dari suatu tindakan yang dapat dihukum.
- 2) Agar sesuatu tindakan dapat dihukum, maka tindakan itu harus memenuhi semua unsur dari delik seperti dirumuskan di dalam undang-undang, dan setiap *strafbaar feit* sebagai pelanggaran terhadap larangan atau kewajiban menurut undang-undang itu yang pada hakikatnya merupakan suatu tindakan melawan hukum atau merupakan suatu *onrechtmatige handeling*.¹⁸

b. Aliran dualisme

Aliran dualisme yaitu aliran yang memisahkan antara unsur-unsur tindak pidana yaitu unsur objektif (unsur perbuatan) dan unsur subjektif (unsur pertanggungjawaban pidana) Andi Zainal Abidin Farid membuat konfigurasi dan membagi unsur-unsur tindak pidana sebagai berikut:¹⁹

- 1) Unsur *Acrus Reus (Delictum)*/ unsur objektif/ unsur perbuatan pidana sebagai berikut:
 - a) Unsur-unsur konstitutif sesuai uraian delik
 - b) Unsur diam-diam
 - 1).Perbuatan aktif atau pasif;
 - 2).Melawan hukum obyektif atau subyektif;
 - 3).Tidak ada dasar pembenar.
- 2) Unsur *Mens Rea*/ unsur subjektif/ unsur pertanggungjawaban pidana sebagai berikut:
 - a) Kemampuan bertanggungjawab

¹⁸ P.A.F.Lamintang, *Op.cit.*, hlm. 184.

¹⁹ Andi Sofyan dan Nur Azisa, 2016, Buku Ajar Hukum Pidana, Pustaka Pena Press, Makassar, hlm. 103-104.

- b) Kesalahan dalam arti luas
 - 1). *Dolus* (kesengajaan),
 - a) Sengaja sebagai niat;
 - b) Sengaja sadar akan kepastian atau keharusan;
 - c) Sengaja sadar akan kemungkinan.
 - 2). *Culpa lata*
 - a) *Culpa lata* yang disadari (alpa);
 - b) *Culpa lata* yang tidak disadari (lalai).

Jadi secara sederhana unsur delik menurut aliran dualisme adalah sebagai berikut:²⁰

- 1) Unsur perbuatan (unsur objektif)
 - a) Perbuatan mencocoki rumusan delik
 - b) Bersifat melawan hukum (tidak ada alasan pembenar)
- 2) Unsur pembuat (unsur subjektif):
 - 1) Dapat dipertanggungjawabkan
 - 2) Ada kesalahan (tidak ada alasan pemaaf)

Menurut van Hamel menunjukkan tiga pengertian perbuatan (*feit*) yakni: ²¹

- a. Perbuatan (*feit*) terjadinya kejahatan (delik). Pengertian ini sangat luas, misalnya dalam suatu kejadian beberapa orang dianiaya, dan apabila dalam suatu penganiayaan dilakukan pula pencurian, maka tidak mungkin dilakukan pula penuntutan salah satu dari perbuatan-perbuatan itu dikemudian dari yang lain.
- b. Perbuatan (*feit*) yang didakwakan ini terlalu sempit contoh seseorang dituntut melakukan perbuatan penganiayaan yang menyebabkan kematian, kemudian masih dapat dilakukan penuntutan atas dasar “sengaja melakukan pembunuhan”

²⁰ *Ibid.*

²¹ E.Y Kanter dan S.R. Sianturi, 2002, *Asas-Asas Hukum Pidana Di Indonesia Dan Penerapannya*, Storia Grafika, Jakarta, hlm. 211.

karena ini lain dari pada “penganiayaan yang mengakibatkan kematian”.

- c. Perbuatan (*feit*) material , jadi perbuatan ini terlepas dari unsur kesalahan dan terlepas dari akibat dengan pengertian ini, maka ketidakpastian yang ada pada kedua pengertian terdahulu dapat dihindari.

Jika salah satu unsur tersebut tidak ada atau lebih tegas tidak terbukti, maka harus disimpulkan bahwa tindak pidana belum atau tidak terjadi. Boleh jadi tindakan sudah terjadi, tetapi bukan suatu tindakan yang terlarang oleh undang-undang terhadap mana diancamkan suatu pidana. Mungkin pula suatu tindakan telah terjadi sesuai dengan perumusan tindakan dalam pasal yang bersangkutan, tetapi tidak terdapat kesalahan pada petindak, dan/ atau tindakan itu tidak bersifat melawan hukum. Berdasarkan hal di atas maka dapat ditarik kesimpulan bahwa:²²

- a. Tiada pidana tanpa terjadi suatu tindakan yang terlarang dan diancam dengan pidana oleh undang-undang;
- b. Tiada pidana, tanpa kesalahan;
- c. Tiada pidana, tanpa sifat melawan hukum;
- d. Tiada pidana, tanpa adanya subjek;
- e. Tiada pidana, tanpa adanya objek.

²² *Ibid.*

3. *Cyber Space*

Cyber space atau dunia maya merupakan hasil integrasi dari media elektronik dan peralatan teknologi jaringan komunikasi yang terhubung dengan peralatan komunikasi yang tersebar diseluruh penjuru dunia dan digunakan untuk keperluan berkomunikasi secara online. pengertian *cyberspace* berasal dari kata *cybernetics* dan *space*, kata ini pertama kali diperkenalkan oleh penulis novel fiksi ilmiah, Wiliam Gibson dalam buku ceritanya, *burning chrome* tahun 1982 dan menjadi populer pada tahun 1984 yang menyebutkan bahwa:²³

“Cyberspace A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts... A graphic representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data. Like city lights, receding”.

Berdasarkan jurnal ‘masyarakat informasi dan digital’ yang ditulis Yasraf Amir Piliang, *cyberspace* adalah sebuah ‘ruang imajiner’, yang didalamnya setiap orang dapat melakukan apa saja yang bisa dilakukan dalam kehidupan sosial sehari-hari dengan cara yang baru, yaitu cara artifisial. Cara artifisial adalah cara yang menitikberatkan pada peran teknologi, khususnya

²³ Yasraf Amir Piliang, “Masyarakat Informasi dan Digital”, Jurnal Socioteknologi Edisi 27, Institut Teknologi Bandung, Desember 2012, hlm. 145.

teknologi komputer dan informasi dalam mendefinisikan realitas sehingga berbagai kegiatan yang dilakukan di dalamnya.²⁴

Cyber space juga dapat dipandang sebagai sebuah dunia komunikasi berbasis komputer yang membuat realitas baru yang sering dikenal dengan sebutan internet. Realitas baru ini dalam kenyataannya terbentuk melauli jaringan komputer yang menghubungkan antar negara atau antar benua yang berbasis *transmission control protocol/internet protocol*.²⁵

Pada perundang-undangan di Indonesia memakai istilah informasi elektronik dan transaksi elektronik dengan pengertian sebagai berikut:²⁶

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

²⁴ *Ibid.*

²⁵ Maskun, 2013, *Kejahatan Siber (CYBER CRIME)*, Kencana Perana Media Group., Jakarta, hlm. 46.

²⁶ Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Transaksi Elektronik Pasal 1 Angka 1-2.

b. Transaksi Elektronik adalah perbuatan hukum yang dilakukan dengan menggunakan komputer, jaringan komputer, dan/ atau media elektronik lainnya.

4. **Cyber Crime**

Cyber crime, computer crimes, konvergensi (kejahatan telematika) dan beberapa istilah lainya yang merujuk pada kejahatan *cyber*. banyaknya istilah ini didasari pada argumentasi bahwa *cyber crime* merupakan kegiatan yang memanfaatkan komputer sebagai media yang didukung oleh sistem telekomunikasi baik itu *dial up system*, yang menggunakan antena khusus yang nirkabel.²⁷ Sebagaimana yang dijelaskan di atas maka yang dimaksud dengan kejahatan *cyber crime, computer crimes*, kejahatan telematika adalah kejahatan dengan arti yang sama dengan penamaan dan penyebutan yang berbeda, maka demi konsistensi penulisan, penulis akan menggunakan istilah *cyber crime*.

Dalam beberapa kepustakaan, *cyber crime* sering identik dengan *computer crime*, menurut *the U.S. Department of justice*, *computer crime* sebagai: “*any illegal act requiring knowledge of computer technology for its perpetration, investigation, or prosecution.*” Pendapat lain dikemukakan oleh *Organization for Economic Cooperation Development (OECD)* yang menggunakan

²⁷ Maskun, *Op.cit*, hlm. 45.

istilah *computer related crime* yang berarti: “*Any illegal, unethical or unauthorized behavior involving automatic data processing and/or transmission data.*”²⁸

Dari pandangan Indra Safitri yang mengemukakan bahwa kejahatan dunia maya adalah jenis kejahatan yang berkaitan dengan pemanfaatan sebuah teknologi informasi tanpa batas serta memiliki karakteristik yang kuat dengan sebuah rekayasa teknologi yang mengandalkan kepada tingkat keamanan yang tinggi dan kredibilitas dari sebuah informasi yang disampaikan dan diakses oleh pelanggan internet.²⁹

Dari pandangan Ibrahim Fikma Edrisy kejahatan siber merupakan keseluruhan bentuk kejahatan yang ditujukan terhadap komputer, jaringan komputer dan para penggunanya, dan bentuk-bentuk kejahatan tradisional yang menggunakan atau dengan bantuan komputer.

Dapat disimpulkan bahwa kejahatan siber adalah setiap aktivitas seseorang, kelompok orang, dan badan hukum yang menggunakan komputer sebagai sarana melakukan kejahatan, dan komputer sebagai sasaran kejahatan.³⁰

Menarik pengertian dari dunia internasional maka didapatkan dua dokumen kongres PBB yang dikutip oleh Barda Nawawi Arief, mengenai *The Prevention of Crime and the Treatment of Offenders* di Havana Cuba pada tahun 1990 dan di Wina Austria pada tahun 2000, menjelaskan adanya dua istilah yang terkait dengan pengertian *Cyber crime*, yaitu *cyber crime* dan

²⁸ *Ibid.*, hlm. 47.

²⁹ Maskun, dkk, 2020, Korelasi Kejahatan Siber Dan Kejahatan Agresi Dalam Perkembangan Hukum Internasional, Nas Media Pustaka, Makassar, hlm. 24.

³⁰ Ibrahim Fikma Edrisy, 2019, Pengantar Hukum Siber, Sai Wawai Publishing, Lampung, hlm. 2-3.

computer related crime. dalam *background paper* untuk lokakarya kongres PBB X/2000 di wina Austria, istilah *cyber crime* di bagi dalam dua kategori. Pertama, *cyber crime* dalam arti sempit (*in a narrow sense*) disebut *computer crime*. kedua, *cyber crime* dalam arti luas (*in a broader sense*) disebut *computer related crime*. ditulis secara lengkap sebagai berikut.³¹

1. *Cyber crime in a narrow sense (computer crime): any legal behaviour directed by means of electronic operations that targets the security of computer system and the data processed by them.*
2. *Cyber crime in a broader sense (computer related crime): any illegal behaviour committed by means on in relation to, a computer system or network, including such crime as illegal possession, offering or distributing information by means of a computer system or network.*

Perlu diketahui istilah *cyber crime* saat ini merujuk pada suatu aktivitas kejahatan yang berhubungan dengan dunia maya (*cyberspace*). secara umum pengertian *cybercrime* adalah perbuatan tanpa izin dan melawan hukum dengan menggunakan komputer sebagai fasilitas utama atau target untuk melakukan

³¹ Barda Nawawi Arief, 2007, Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan, Kencana Perdana Media Group, Jakarta, hlm. 8.

kejahatan, dengan atau tanpa merubah data atau merusak sistem komputer yang digunakan.³²

Dalam peraturan *the proposed west virginia computer crimes act* adalah:

“an electronic, magnetic, optical, electrochemical or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable handheld calculator, or other similar device”.

Mengenai pengertian kejahatan komputer menurut peraturan perundang-undangan di virginia dapat dipahami bahwa sesuatu yang berhubungan dengan peralatan pemrosesan data listrik, *magnetic, optic*, elektro kimia, atau peralatan kecepatan tinggi lainnya dalam melakukan logika aritmatika, atau fungsi penyimpanan dan memasukkan beberapa fasilitas penyimpanan data atau fasilitas komunikasi yang secara langsung berhubungan dengan operasi tersebut dalam konjungsi dengan peralatan tersebut tidak memasukkan mesin ketik otomatis atau pengatur waktu, sebuah kalkulator tangan atau perlatan serupa lainnya.³³

Penulis sependapat dengan pengertian yang dikemukakan oleh Fredy AH Sihombing yang mengartikan bahwa *cyber crime* merupakan bentuk kejahatan yang timbul karena memanfaatkan

³² Dikdik dan Elisatris, 2009, *Cyber Law* Aspek Hukum Teknologi Informasi, Bandung, Refika Aditama, hlm. 8.

³³ Abdul Wahid dan Mohammad Labib, 2005, *Kejahatan Mayantara (Cyber Crime)*, Jakarta, PT. Refika Aditama, hlm. 41.

teknologi internet, yang sejalan dengan kemajuan teknologi informasi muncul beberapa kejahatan yang mempunyai karakteristik. Kejahatan tersebut adalah kejahatan yang timbul akibat penyalahgunaan jaringan internet (kejahatan dunia maya/*cyber crime*).³⁴

Dalam beberapa literatur masih banyak pula yang menggunakan istilah komputer, penggunaan istilah komputer dalam pengertian *cybercrime* tentu saja tidak salah namun pada zaman modern ini istilah komputer tentu saja berbeda, kejahatan yang dulu nya hanya bisa dilakukan dengan komputer sekarang dapat dilakukan dengan gawai pintar atau *smartphone*. Hal ini tak lepas dari perkembangan teknologi yang sangat cepat, membuat hukum tertatih mengejar perkembangan teknologi, hukum sangat dibutuhkan bagi manusia agar terjaminnya pemenuhan hak warga negara, jaminan keamanan, dan stabilitas kehidupan masyarakat luas, maka dari itu perlunya hukum mengikuti perkembangan teknologi.

5. Jenis-Jenis *Cyber Crime*

Pada pembahasan sebelumnya telah kita ketahui bahwa banyak pendapat dari para ahli hukum ataupun dari produk hukum itu sendiri tentang bagaimana itu *cyber crime*. Suatu alasan mendasar para ahli hukum berbeda pendapat mengenai apa itu

³⁴Sastya Hendri Wibowo, (et.al), 2022, *Cyber Crime di Era Digital*, Padang, PT. Global Eksekutif Teknologi, hlm. 139.

cyber crime, membuat banyaknya perbedaan tentang apa saja jenis-jenis dari *cyber crime* itu sendiri. Penulis akan mencoba merangkum apa saja jenis-jenis *cyber crime* dari beberapa sumber sebagai berikut:

a. *Illegal Access*

Jika penulis dapat mengutip dari *council of europe* yang dimaksud sebagai *illegal access* adalah sebagai berikut:

*“Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.”*³⁵

Dapat penulis terjemahkan secara bebas sebagai berikut: pihak negara harus menerapkan undang-undang dan mengambil tindakan-tindakan lain yang diperlukan untuk ditetapkan sebagai tindak pidana, mengakses secara sadar seluruh atau sebagian dari sistem komputer tanpa hak. Pihak negara berhak mensyaratkan bahwa pelanggaran langkah-langkah pengamanan dengan maksud mengambil data komputer atau untuk niat lain yang tidak jujur, atau berkaitan dengan sebuah sistem komputer yang tersambung kepada sistem komputer lainnya.

³⁵ *Council Of Europe, 2001, European Treaty Series No. 185 Chapter II Measures To Be Taken At The Nation Level, Budapest, hlm. 3.*

Illegal access melingkupi pelanggaran dasar dari ancaman-ancaman yang berbahaya dari serangan terhadap keamanan data dan sistem komputer.³⁶ Pada pasal ini juga menerangkan mengenai pentingnya permasalahan tanpa hak yang harus ada pada suatu pelanggaran yang dilakukan, bukanlah suatu pelanggaran pidana terhadap akses yang disetujui oleh pemilik atau pemegang hak dari suatu sistem atau bagian dari pemilik atau pemegang hak tersebut.³⁷

b. *Illegal Interception*

Seperti pada pengertian sebelumnya penulis dapat mengutip dari *council of europe* yang dimaksud sebagai *illegal interception* adalah sebagai berikut:

*“Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.”*³⁸

Dapat diartikan seperti berikut: “pihak negara harus menerapkan undang-undang dan mengambil tindakan-tindakan lain sebagaimana mungkin perlu untuk ditetapkan sebagai tindak pidana, menyadap tanpa hak, melalui teknik-teknik tertentu, transmisi data komputer yang bukan milik umum, dari atau dalam sebuah sistem komputer, termasuk

³⁶ Council Of Europe, *Explanatory Report To The Convention On Cybercrime (ets no185)*, poin. 144.

³⁷ *Ibid.*, poin 47.

³⁸ Council of Europe, *Loc.cit.*

emisi elektromagnetik dari sebuah sistem komputer yang membawa data komputer tersebut. Pihak negara dapat mensyaratkan bahwa tindakan-tindakan tersebut dilakukan dengan tujuan yang tidak jujur, berkaitan dengan sistem komputer yang tersambung kepada sistem komputer lain.”

Intersepsi dengan cara teknis berhubungan dengan mendengarkan, memantau atau mengawasi isi komunikasi, untuk mendapatkan isi data baik secara langsung, melalui akses dan penggunaan sistem komputer, atau secara tidak langsung, melalui penggunaan elektronik, penyadapan atau perangkat penyadapan. Intersepsi juga dapat melibatkan perekaman. Sarana teknis termasuk perangkat teknis yang dipasang pada saluran transmisi serta perangkat untuk mengumpulkan dan merekam komunikasi nirkabel. Ini mungkin termasuk penggunaan perangkat lunak, kata sandi dan kode. Persyaratan penggunaan sarana teknis adalah kualifikasi yang ketat untuk menghindari kriminalisasi yang berlebihan.³⁹

c. *Data Interference/ Data Forgery*

Dalam beberapa kepustakaan yang bersumber dari *council of europe* yang dimaksud *data interference* adalah pihak negara harus menerapkan undang-undang dan mengambil tindakan-tindakan lain yang di perlukan untuk ditetapkan sebagai tindak pidana, pengrusakan, penghapusan,

³⁹ *Council of europe, Op.cit., poin. 53.*

pemburukan, perubahan, atau menahan data komputer tanpa hak dan dengan sengaja. Seperti yang tercantum pada *council of europe* seperti berikut ini:

“Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.”⁴⁰

Ketentuan pengrusakan data menjadi tindak pidana bertujuan untuk memberikan perlindungan yang sama terhadap data komputer dan program computer sebagaimana dengan benda-benda berwujud. Sebagai contoh adalah memasukan kode-kode jahat (*malicious codes*), *Viruses*, dan *Trojan Horse* kepada suatu sistem komputer merupakan pelanggaran menurut ketentuan pasal ini.⁴¹

d. *System Interference*

Seperti yang diatur dalam *council of europe* menetapkan bahwa pihak negara harus menerapkan undang-undang dan mengambil tindakan-tindakan lain yang diperlukan untuk ditetapkan sebagai tindak pidana, secara serius merintangi fungsi dari sebuah sistem komputer dengan tanpa hak melalui memasukkan, memindahkan, merusak, menghapus, memperburuk, mengubah atau menahan data komputer”. dalam pasal ini disebutkan bahwa harus dilakukan dengan

⁴⁰ *Council of Europe, Op.cit.*, hlm. 4.

⁴¹ Mike Keyser, *The Council of Europe Convention on Cybercrime, Journal of Transnational Law and Policy*, vol. 12, 2003, hlm. 302.

memasukkan, menyebarkan, merusak, menghapus atau menyembunyikan data komputer. Seperti yang akan penulis kutip secara langsung seperti berikut: ⁴²

“Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.”

System interference bisa dikatakan sebagai suatu serangan, gangguan, atau rintangan serius tanpa hak terhadap penghapusan, perubahan, dan berfungsinya suatu sistem komputer.

e. *Unauthorized Access to Computer System and Service*

Merupakan kejahatan yang dilakukan kedalam suatu sistem jaringan komputer secara tidak sah, tanpa izin, atau tanpa sepengetahuan dari pemilik sistem jaringan komputer yang dimasukinya. Biasanya pelaku kejahatan (*hacker*) melakukannya dengan maksud sabotase ataupun pencurian informasi penting dan rahasia. Namun begitu, ada juga yang melakukannya hanya karena merasa tertantang untuk mencoba keahliannya menembus suatu sistem yang memiliki tingkat proteksi tinggi. Kejahatan seperti ini semakin sering terjadi dikarenakan perkembangan teknologi internet. ⁴³

⁴² Council of Europe, *Op.cit.*, hlm. 4.

⁴³ Maskun, *Op.cit.*, hlm. 51.

f. **Illegal Contents**

Kejahatan yang dilakukan dengan memasukkan data atau informasi kepada internet tentang sesuatu hal yang tidak benar, tidak etis, dan dianggap melanggar hukum atau mengganggu ketertiban umum. Sebagai contoh adalah:⁴⁴

- 1) Pemuatan suatu berita bohong atau fitnah yang akan menghancurkan martabat atau harga diri pihak lain.
- 2) Pemuatan hal-hal yang berhubungan dengan pornografi.
- 3) Pemuatan suatu informasi yang merupakan rahasia negara, agitasi, dan propaganda untuk melawan pemerintah yang sah, dan sebagainya.

g. *Cyber Espionage*

Kejahatan ini memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer (*computer network system*) pihak sasaran. Kejahatan ini biasanya ditujukan terhadap saingan bisnis yang dokumen ataupun data-data pentingnya tersimpan dalam suatu sistem komputerisasi.⁴⁵

h. *Cyber Sabotage and Extoriton*

Merupakan kejahatan yang dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang

⁴⁴ *Ibid.*, hlm. 52.

⁴⁵ *Ibid.*, hlm. 52-53

tersambung dengan internet. Biasanya kejahatan ini dilakukan dengan menyusupkan suatu *logic bomb*, Virus komputer, atau pun suatu program tertentu sehingga data program komputer atau sistem jaringan komputer tidak dapat digunakan atau tidak berjalan sebagaimana yang dikehendaki oleh pelaku. Dalam beberapa kasus setelah hal tersebut terjadi maka pelaku kejahatan tersebut menawarkan diri kepada korban untuk memperbaiki data, program komputer atau sistem jaringan komputer yang telah disabotase, tentunya dengan bayaran tertentu. ⁴⁶

i. *Offence Against Intellectual Property*

Kejahatan yang ditujukan terhadap hak kekayaan intelektual yang dimiliki seseorang di internet. Sebagai contoh adalah peniruan tampilan *web page* suatu situs milik orang lain secara illegal, penyiaran suatu informasi di internet yang ternyata merupakan rahasia dagang orang lain, dan sebagainya. ⁴⁷

j. *Infringements of Privacy*⁴⁸

Kejahatan ini ditujukan terhadap informasi seseorang yang merupakan hal yang sangat pribadi dan rahasia. Kejahatan ini biasanya di tujukan terhadap keterangan pribadi

⁴⁶ *Ibid.*, hlm. 53.

⁴⁷ *Ibid.*

⁴⁸ *Ibid.*, hlm. 53-54.

seseorang yang tersimpan secara komputerisasi, yang apabila diketahui oleh orang lain, maka dapat merugikan orang secara material maupun imateriel, seperti nomor kartu kredit, nomor pin atm, keterangan tentang cacat atau penyakit tersembunyi, dan sebagainya.

k. *Cyberstalking*⁴⁹

Kejahatan jenis ini dilakukan untuk mengganggu atau melecehkan seseorang dengan memanfaatkan komputer, misalnya menggunakan e-mail dan dilakukan berulang-ulang. Kejahatan tersebut menyerupai teror yang ditujukan kepada seseorang dengan memanfaatkan media internet. Hal itu bisa terjadi karena kemudahan dalam membuat email dengan alamat tertentu tanpa harus menyertakan identitas diri yang sebenarnya.

l. *Hacking and Cracker*⁵⁰

Istilah *hacker* biasanya mengacu pada seseorang yang punya minat besar untuk mempelajari sistem komputer secara detail dan bagaimana meningkatkan kapabilitasnya. Adapun mereka yang sering melakukan aksi-aksi perusakan di internet lazimnya disebut *cracker*. Pendapat ini dapat dikatakan bahwa *cracker* sebenarnya adalah *hacker* yang

⁴⁹ Dodo Zaenal Abidin, "Kejahatan Dalam Teknologi Informasidan Komunikasi", Jurnal Ilmiah Media Processor, STIKOM Dinamika Bangsa, vol. 10, Nomor 2, Oktober 2015, hlm. 511.

⁵⁰ *Ibid.*

memanfaatkan kemampuannya untuk hal-hal yang negatif. Aktivitas *cracking* di internet memiliki lingkup yang sangat luas, mulai dari pembajakan account milik orang lain, pembajakan situs web, *probing*, menyebarkan virus, hingga pelumpuhan target sasaran. Tindakan yang terakhir disebut sebagai *Denial Of Service* selanjutnya disebut DoS. *DoS* attack merupakan serangan yang bertujuan melumpuhkan target (*hang, crash*) sehingga tidak dapat memberikan layanan.

m. *Cybersquatting and Typosquatting*⁵¹

Cybersquatting merupakan kejahatan yang dilakukan dengan mendaftarkan domain nama perusahaan orang lain dan kemudian berusaha menjualnya kepada perusahaan tersebut dengan harga yang lebih mahal. Adapun *typosquatting* adalah kejahatan dengan membuat domain plesetan yaitu domain yang mirip dengan nama domain orang lain. Nama tersebut merupakan nama domain saingan perusahaan.

n. *Cyber Terrorism*⁵²

Suatu tindakan *cybercrime* termasuk *cyber terrorism* jika mengancam pemerintah atau warga negara, termasuk *cracking* ke situs pemerintah atau militer. Beberapa contoh kasus *cyber terrorism* sebagai berikut :

⁵¹ *Ibid.*

⁵² *Ibid.*

- 1) Ramzi Yousef, dalang penyerangan pertama ke gedung WTC, diketahui menyimpan detail serangan dalam file yang dienkripsi dalam laptopnya.
 - 2) Osama Bin Laden diketahui menggunakan *steganography* untuk komunikasi jaringannya.
 - 3) Suatu website yang dinamai *Club Hacker Muslim* diketahui menuliskan daftar tips untuk melakukan *hacking* kepada Pentagon.
 - 4) Seorang *hacker* yang menyebut dirinya sebagai Doktor Nuker diketahui telah kurang lebih lima tahun melakukan *defacing* atau mengubah isi halaman web dengan propaganda anti-American, anti-Israel dan pro-Bin Laden.
- o. *Carding*⁵³

Carding adalah penipuan kartu kredit bila pelaku mengetahui nomor kartu kredit seseorang yang masih berlaku, maka pelaku dapat membeli barang secara online yang tagihannya dialamatkan pada pemilik asli kartu kredit tersebut, sedangkan pelakunya dinamakan *carder*.

Kejahatan *carding* merupakan kejahatan yang memanfaatkan teknologi internet sebagai sarana utama untuk mengakses secara tidak sah suatu sistem sebuah website

⁵³ MOHD. Yusuf DM, Boyke.SM, Rika Parlina, Analisis Kejahatan *Carding* Dalam Bentuk *Cyber Crime* dan Perlindungan Hukum di Indonesia, Jurnal Pendidikan dan Konseling, Fakultas Hukum Universitas Lancang Kuning. Volume 4 Nomor 6 Tahun 2022, hlm. 4205.

untuk mendapatkan data-data para nasabah kartu kredit. Tujuannya adalah untuk membelanjakan secara tidak sah kartu kredit yang telah didapatkan ataupun untuk mendapatkan dana milik pemegang kartu kredit tersebut.

p. *Hijacking*

Hijacking merupakan kejahatan pembajakan hasil karya orang lain. Yang paling sering terjadi adalah *software piracy* (pembajakan perangkat lunak).⁵⁴

B. Tinjauan Umum Mengenai Phising

1. Pengertian Phising

Pertamkali istilah "*phising*" dipublikasikan oleh *american online usernet newgroup* pada tanggal 2 januari 1996 dan mulai menjamur pada tahun 2004.⁵⁵ Istilah *phising* adalah bentuk lain dari kata *phishing* yang berasal dari bahasa inggris '*ishing*' yaitu memancing. Bisa dibilang aktivitas *phising* adalah bertujuan memancing orang untuk memberikan informasi pribadi secara sukarela tanpa disadari untuk tujuan kejahatan, di mana dengan kata lain arti *phising* adalah serangan yang dilakukan untuk menipu atau memancing korban agar mau mengklik link atau

⁵⁴ Dodo Zaenal Abidin, *Loc.cit.*

⁵⁵ Husnul Anwari dan Java Creativity, 2011, Website Hantu, PT. Elex Media Komputindo, Jakarta, hlm. 167.

tautan serta menginput informasi krusial seperti *username* dan *password*.⁵⁶

Pada referensi lain pengertian *Phising* adalah upaya untuk mendapatkan informasi tentang data pribadi dengan menggunakan teknik *phishing*. Data *phishing* mencakup informasi pribadi (nama, alamat, jenis kelamin, tanggal lahir), informasi akun (nama pengguna dan kata sandi), dan informasi keuangan (informasi kartu kredit, akun). Aktivitas *phishing* bertujuan untuk mengelabui orang agar secara sukarela memberikan informasi pribadi tanpa sepengetahuan mereka. Namun informasi yang dibagikan akan digunakan untuk tujuan jahat.⁵⁷

Berbeda dengan modus operandi *hacker* atau kejahatan *cyber crime* lainnya, kejahatan phising terletak pada korban yang tidak sadar telah memakan umpan dari pelaku *phising*, yang intinya ada peran aktif dari korban yang memberikan secara sukarela data pribadinya tanpa paksaan (secara sukarela) dikarenakan psikologis dan teknik menipu dari pelaku lah yang membuat korban termanipulasi. Seperti filosofis dari memancing itu sendiri siapkan umpan, tebar umpan nya, ikan-ikan akan datang dan memakan umpan tersebut, dan pemancing pun

⁵⁶ Hardi Fardiansyah, (Et.Al.), 2022, *Cyber Crime Paling Populer Pada Era Digital*, Media Sains Indonesia, Bandung, hlm. 3.

⁵⁷ Sastya Hendri Wibowo, (et.al), Loc.cit. hlm. 1.

mendapatkan ikan yang dipancing (informasi pribadi korban telah didapatkan).

Dari literatur yang lain pula ada yang mengkaitkan dengan modus penipuan di dunia internet/ *cyber space*. Dengan pengertian *Phising* adalah salah satu kejahatan elektronik dalam bentuk penipuan, di mana proses *phising* ini bermaksud untuk menangkap informasi yang sangat sensitif seperti username, *password* dan detil kartu kredit dalam bentuk meniru sebagai sebuah entitas yang dapat dipercaya/*legitimate organization* dan biasanya berkomunikasi secara elektronik.⁵⁸

Pelaku *phising* dikenal dengan sebutan *phiser*.⁵⁹ Berbeda dengan para *hacker* yang pertama kali kemunculannya dianggap sebagai arti positif untuk menyebut seorang anggota yang memiliki keahlian dalam bidang komputer dan mampu membuat program komputer yang lebih baik daripada yang telah dirancang bersama. Sedangkan *phiser* dari awal kemunculan nya sudah memiliki konotasi yang negatif, ini dikarenakan adanya istilah *white hat hacker* yang secara umum lebih memfokuskan aksinya

⁵⁸ Dian Rachmawati, "Phising Sebagai Salah Satu Bentuk Ancaman dalam Dunia Cyber," *Jurnal Saintkom*, Vol. 13, No. 3, 2014, hlm. 211.

⁵⁹ Hardi Fardiansyah,(et.al.), Loc.cit., hlm. 5.

bagaimana melindungi sebuah sistem.⁶⁰ Dengan kata lain mencari dan memperbaiki kelemahan dari suatu sistem.

2. Jenis-Jenis Phising

Dalam modus operandi *phising* pun terdapat beberapa cara yang dilakukan oleh para phiser sebagai berikut:

a. *Email Phising*⁶¹

Cara ini cukup populer untuk menjerat korban, *phiser* akan mengirimkan sebuah e-mail palsu, dimana phiser seolah-olah adalah petugas ataupun admin website suatu perusahaan perbankan. Bagaimana phiser mendapatkan e-mail para korbannya kemungkinan berasal dari *searching* internet ataupun data pribadi yang bocor dan diperjual bebas di internet, mendapat keterangan dari kartu nama, melihat dari anggota *mailing list*, dan sebagainya. Isi e-mail palsu tersebut biasanya seputar pemberitahuan kepada nasabahnya tentang suatu hal tertentu yang sifatnya penting, mendesak, dan membutuhkan respon cepat.

Untuk membuat korban percaya, maka tampilan e-mail palsu tersebut di desain semirip e-mail aslinya, dengan bahasa, kop surat, logo, dan sebagainya. Untuk semakin memudahkan

⁶⁰ Ricardi Hermawan, 2009, *The Drop Out Billionaire* Menjual Ide Ala Mark Zuckerberg, Best Publisher, Yogyakarta, hlm. 17.

⁶¹ Ki Jagad Tomara, 2011, "*Kajian Yuridis Pertanggungjawaban Pidana Penyedia Jasa Internet dan Pemilik Domaini Situs Phising*", Skripsi, Fakultas Hukum Universitas Brawijaya, Malang, hlm. 54.

korban terjerat dalam *e-mail* palsu tersebut dicantumkan suatu *hyperlink* yang diharapkan diklik oleh korban, yang apabila diklik akan menuntun korban ke suatu halaman web yang juga sudah dirancang sedemikian rupa oleh *phisher*.

b. *Spear Phising*⁶²

Merupakan jenis *e-mail phising*, perbedaannya adalah bahwa alih-alih mengirim e-mail massal kepada calon korban secara acak, *spear phising* menargetkan calon korban tertentu. Teknik ini biasanya dilakukan setelah mendapatkan informasi dasar tentang calon korban, seperti nama dan alamat.

c. *Whaling*

Whaling adalah serangan *phising* yang menargetkan tidak hanya individu, tetapi juga individu yang sangat istimewa dalam organisasi seperti perusahaan, manager sumber daya manusia dll oleh karena itu, jika operasi penangkapan ikan paus ini berhasil, akan ada banyak manfaat dari akses yang diperoleh.⁶³ Contoh kasus dari *whaling* ini pernah terjadi di amerika pada tahun 2016, peretas menyamar menjadi CEO *Crelan Bank* untuk meminta karyawan mengirimkan sejumlah uang ke rekeningnya. Mengingat e-mail tersebut dikirimkan oleh CEO, para karyawan tidak menaruh curiga, dana pun

⁶² Sastya Hendri Wibowo, (et.al), Loc.cit., hlm. 3.

⁶³ *Ibid.*

dikirimkan ke rekening *phiser*. *Phising* ini terkuak setelah adanya internal audit dari *Crelan Bank*, *Crelan Bank* pun melaporkan bahwa mengalami kerugian hingga 75 juta dollar karena kasus ini.⁶⁴

d. *Web Phising/ Web Forgery*

web phising adalah upaya untuk mengelabui calon korban menggunakan situs web palsu. Situs web *phising* terlihat seperti situs web resmi dan menggunakan nama domain yang serupa, ini disebut *spoofing domain*.⁶⁵

Web forgery adalah *website* atau situs yang sengaja dirancang untuk menipu pengunjungnya. Hal ini sering dikenal dengan istilah *pharming*. *pharming* berasal dari kata dalam bahasa Inggris, *farming* yang berarti memanen. Cara ini diawali dengan pelaku menghost sebuah domain dalam dunia maya, dapat melalui *web hosting* gratis yang dapat dengan mudah ditemui di internet, maupun jasa *web hosting* yang disediakan oleh perusahaan penyedia jasa internet. Kemudian setelah mendapatkan domain tersebut, pelaku akan merancang sebuah *website*. Tampilan *website* ini akan dibuat semirip aslinya baik tata letak, logo perusahaan, kata-kata, huruf (jenis, ukuran, warna), maupun objek yang disertakan (gambar,

⁶⁴ Asia Quest Indonesia, *Loc, cit.*

⁶⁵ Sastya Hendri Wibowo, (et.al), *Loc. cit.*

suara, maupun animasi) pada *website*. Kemudian korban akan dituntun untuk memasukkan identitasnya melalui suatu form isian yang sudah disiapkan oleh pelaku *phiser*. Setelah korban memasukkan *user id* dan *password*-nya, maka data akan tersimpan dalam *database website* palsu tersebut, dan pelaku *phising* hanya akan tinggal 'memanen' data-data tersebut untuk kemudian disalahgunakan.⁶⁶

e. *Phising* Melalui Telepon (*Phone Phising*)

Cara ini merupakan pengembangan dari teknik *phising* secara konvensional. Hanya saja teknik ini lebih banyak menggunakan media telepon daripada internet. Pelaku akan menelpon pihak yang berwenang dengan menggunakan nama seorang dengan menggunakan kedok tertentu. Umumnya kedok yang digunakan pelaku antara lain sebagai *user* penting, kedok sebagai *user* yang sah, kedok sebagai mitra *vendor*, kedok sebagai konsultan audit, kedok sebagai penegak hukum, dan sebagainya.⁶⁷ Contoh dari peristiwa *phising*, dimana *phiser* menggunakan kedok sebagai penegak hukum "selamat sore pak, kami dari kepolisian yang bekerja sama dengan tim keamanan internet nasional. Hasil monitoring kami memperlihatkan sedang ada serangan menuju server anda dari luar negeri. Kami bermaksud untuk melindunginya. Bisa minta

⁶⁶ Ki Jagad Tomara, *Op.cit.*, hlm. 56.

⁶⁷ *Ibid.*, hlm. 57.

tolong diberikan perincian kepada kami mengenai topologi dan spesifikasi jaringan anda secara detail?”. Tentu saja yang bersangkutan biasanya langsung memberikan informasi penting tersebut karena merasa takut untuk menanyakan keabsahan atau keaslian identitas penelpon.⁶⁸

f. *Phising Melalui SMS (SMS Phising)*⁶⁹

Telepon genggam merupakan sebuah teknologi yang cukup fenomenal. Dalam beberapa waktu saja penggunaannya sudah menunjukkan kenaikan penjualan nomor selular. Fakta ini rupanya juga tak luput dimanfaatkan oleh para kriminal dalam melakukan tindak kejahatan. Melalui metode pengiriman sebuah *sms* kepada korban. Bagaimana cara pelaku mendapatkan nomor korban? Dengan menjamurnya *counter-counter* penjualan pulsa, maka mendapatkan nomor telepon selular seseorang bukanlah suatu hal yang sulit. Isi dari *sms* tersebut umumnya berisi ucapan yang hadiahnya umumnya berupa uang dengan nominal yang relatif besar. Untuk dapat mengambil hadiah tersebut, korban diharapkan mengkonfirmasi dengan cara memberikan user id dan *password* internet bankingnya kepada pelaku.

Contoh dari kasus sms phising seperti berikut:

⁶⁸ *Ibid.*, hlm. 59-60.

⁶⁹ *Ibid.*, hlm. 60-61.

“selamat. Anda baru saja memenangkan hadiah sebesar Rp25,000,000 dari bank X yang bekerjasama dengan provider telekomunikasi Y. Agar kami dapat segera mentransfer uang tunai kemenangan ke rekening bank anda, mohon diinformasikan user name dan password internet bank anda kepada kami. Sekali lagi kami atas manajemen bank X mengucapkan selamat atas kemenangan anda...”

g. *Phising* Melalui Aplikasi Percakapan (*Chat Phising*)⁷⁰

Dalam cara ini, pelaku akan menyiapkan sebuah program otomatis. Program ini dapat disisipkan pada aplikasi *chatting* populer seperti *Yahoo! Messenger*, *MSN Messenger*, dan lain sebagainya. Cara ini juga dapat ditemui pada layanan *customer service online* sebuah perusahaan. *Customer service online* adalah sebuah layanan yang disediakan oleh perusahaan kepada pelanggannya apabila terjadi suatu keluhan atau permasalahan, ataupun sekedar mencari informasi secara online. Umumnya suatu *customer service online* berbasis *chatting*. Apabila disisipkan pada sebuah aplikasi *chatting* (dalam contoh ini menggunakan *yahoo! Messenger*), maka pelaku akan menampilkan sebuah pesan pada korbannya dengan disertai sebuah *hyperlink*.

Pesan tersebut biasanya berisi tentang seseorang yang telah mengunggah suatu gambar yang akan membuat korban merasa penasaran. Untuk mengetahui gambar tersebut, maka korban diharuskan mengklik *hyperlink* yang tersedia. Namun

⁷⁰ *Ibid.*, hlm. 61-63.

setelah *hyperlink* tersebut diklik, bukannya gambar yang dimaksud yang keluar, tapi tampilan yang menyatakan ia harus *log in* kembali agar dapat mengakses gambar tersebut. Apabila korban terpancing pada jebakan tersebut, maka ia akan memasukkan *user id* beserta *password*-nya, dan tercapailah tujuan si pelaku.

C. Pemahaman Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Informasi Dan Transaksi Elektronik

1. Pengertian informasi elektronik dan transaksi elektronik

Pada Pasal 1 angka (1) UURI ITE 2016 yang dimaksud dengan informasi elektronik adalah:

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

Berpedoman pada undang-undang ite pada pasal 1 angka (2) yang dimaksud transaksi elektronik ialah:

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

2. Klasifikasi Tindak Pidana *Phising* Menurut UURI ITE 2016

pengaturan tindak pidana phising menurut UURI ITE 2016 diatur dalam beberapa pasal yang pertama terdapat pada pasal 32 Ayat (1):

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

Pengaturan mengenai ancaman tindak pidana diatur dalam pasal 48 ayat (1) UURI nomor 19 tahun 2016 tentang perubahan atas undang-undang nomor 11 tahun 2008 tentang informasi dan transaksi elektronik :

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

Dalam praktiknya jaksa akan memberikan pasal alternatif dengan pasal 30 ayat 1, pasal 32 ayat 2 dan pasal 35 jika dalam modus operandi *phising* itu dilakukan tindak kejahatan lanjutan dengan bunyi pasal seperti berikut:

“pasal 30 ayat 1: setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik milik orang lain dengan cara apa pun.

pasal 32 Ayat (2): Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik Orang lain yang tidak berhak.

pasal 35: Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik.”

Pengaturan mengenai ancaman tindak pidana pasal 30 ayat 1 diatur dalam pasal 46, pasal 32 ayat 2 diatur dalam pasal 48 ayat 2 dan pasal 35 diatur dalam pasal 51 ayat (1) UURI nomor 19 tahun 2016 tentang perubahan atas undang-undang nomor 11 tahun 2008 tentang informasi dan transaksi elektronik :

“pasal 46 ayat (1) : setiap orang yang memenuhi unsur sebagaimana dimaksud dengan pasal 30 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp600.000.000,00 (enam ratus juta rupiah)

Pasal 48 Ayat (2): setiap orang yang memenuhi unsur sebgaimana dimaksud dalam pasal 32 ayat (2) dipidana dengan pidana penjara paling lama 9 (sembilan) tahun dan/atau denda paling banyak Rp3.000.000.000,00 (tiga miliar rupiah).

Pasal 51 Ayat (1): Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 35 dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp12.000.000.000,00 (dua belas miliar rupiah).

D. Pemahaman Undang-Undang Republik Indonesia Nomor 27

Tahun 2022 Tentang Perlindungan Data Pribadi

1. Pengertian Data Pribadi Dan Perlindungan Data Pribadi

Berpedoman pada pasal 1 angka (1) UURI PDP 2022 tentang perlindungan pribadi yang dimaksud dengan data pribadi adalah sebagai berikut:

“data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik atau nonelektronik.”⁷¹

Bersumber pada pasal 1 angka (2) UURI nomor 27 tahun 2022 tentang perlindungan data pribadi sebagai berikut:

“perlindungan data pribadi adalah keseluruhan upaya untuk melindungi data pribadi dalam rangkaian pemrosesan data pribadi guna menjamin hak konstitusional subjek data pribadi.”⁷²

2. Asas Dan Penjelasanya

Pada bab II pasal 3 UURI nomor 27 tahun 2022 tentang perlindungan data pribadi di sebutkan asas apa saja sebagai berikut:

“Undang-Undang ini berasaskan :⁷³

- a. perlindungan;
- b. kepastian hukum;
- c. kepentingan umum;
- d. kemanfaatan;

⁷¹ Undang-undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi Pasal 1 Angka 1.

⁷² *Ibid.*, Pasal 1 Angka 2.

⁷³ *Ibid.*, pasal 3.

- e. kehati-hatian;
- f. keseimbangan;
- g. pertanggungjawaban; dan
- h. kerahasiaan.”

Pada lembar penjelasan dijelaskan poin-poin pada asas ini sebagai berikut :⁷⁴

“Penjelasan asas meliputi:

- a. Yang dimaksud dengan "asas perlindungan" adalah bahwa setiap pemrosesan Data Pribadi dilakukan dengan memberikan perlindungan kepada Subjek Data Pribadi atas Data Pribadinya dan Data Pribadi tersebut agar tidak disalahgunakan.
- b. Yang dimaksud dengan "asas kepastian hukum" adalah bahwa setiap pemrosesan Data Pribadi dilakukan berdasarkan landasan hukum untuk mewujudkan Pelindungan Data Pribadi serta segala sesuatu yang mendukung penyelenggaraannya sehingga mendapatkan pengakuan hukum di dalam dan di luar pengadilan.
- c. Yang dimaksud dengan "asas kepentingan umum" adalah bahwa dalam menegakkan Pelindungan Data Pribadi harus memperhatikan kepentingan umum atau masyarakat secara luas. Kepentingan umum tersebut antara lain kepentingan penyelenggaraan negara dan pertahanan dan keamanan nasional.
- d. Yang dimaksud dengan "asas kemanfaatan" adalah bahwa pengaturan Pelindungan Data Pribadi harus bermanfaat bagi kepentingan nasional, khususnya dalam mewujudkan cita-cita kesejahteraan umum.
- e. Yang dimaksud dengan "asas kehati-hatian" adalah bahwa para pihak yang terkait dengan pemrosesan dan pengawasan Data Pribadi harus memperhatikan segenap aspek yang berpotensi mendatangkan kerugian.
- f. Yang dimaksud dengan “asas keseimbangan” adalah sebagai upaya Pelindungan Data Pribadi untuk menyeimbangkan antara hak atas Data Pribadi di satu pihak dengan hak negara yang sah berdasarkan kepentingan umum.
- g. Yang di maksud dengan “asas pertanggungjawaban” adalah bahwa semua pihak yang terkait dengan pemrosesan dan pengawasan data pribadi bertindak

⁷⁴ *Ibid.*, penjelasan pasal 3.

secara bertanggungjawab sehingga mampu menjamin keseimbangan hak dan kewajiban para pihak terkait termasuk subjek data pribadi.

- h. Yang dimaksud dengan “asas kerahasiaan” adalah bahwa data pribadi terlindungi dari pihak yang tidak berhak dan/atau dari kegiatan pemrosesan data pribadi yang tidak sah.”

3. klasifikasi tindak pidana phishing menurut UURI PDP

Kualifikasi menurut UURI PDP 2022 tentang perlindungan data pribadi pasal 65 angka (1) dan angka (3):

“Angka (1): Setiap Orang dilarang secara melawan hukum memperoleh atau mengumpulkan Data Pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian Subjek Data Pribadi.

Angka (3):Setiap orang dilarang secara melawan hukum menggunakan Data pribadi yang bukan miliknya.”

Pengaturan mengenai ancaman tindak pidana phishing menurut pasal 67 angka (1) UURI nomor 27 tahun 2022 tentang perlindungan data pribadi:

Angka (1): Setiap Orang yang dengan sengaja dan melawan hukum memperoleh atau mengumpulkan Data Pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian Subjek Data Pribadi sebagaimana dimaksud dalam Pasal 65 ayat (1) dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau pidana denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah).

Angka (3): Setiap Orang yang dengan sengaja dan melawan hukum menggunakan Data Pribadi yang bukan miliknya sebagaimana dimaksud dalam Pasal 65 ayat (3) dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau pidana denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah).

E. Tinjauan Umum Yurisdiksi Dalam Tindak Pidana Phising

1. Pengertian Yurisdiksi

Terdapat beberapa istilah mengenai yurisdiksi seperti jurisdiction, hak menurut hukum, kekuasaan menurut hukum, dan kewenangan menurut hukum dan sebagainya. Yurisdiksi berasal dari bahasa Inggris 'jurisdiction'. *Jurisdiction* berasal dari bahasa Latin yaitu 'jurisdictio' yang terdiri dari kata 'juris' yang berarti "kepunyaan menurut hukum", dan 'diction' yang berarti yang berarti "ucapan, sabda, sebutan, firman". Dengan demikian, yurisdiksi berarti kepunyaan seperti yang ditentukan oleh hukum, hak menurut hukum, kekuasaan menurut hukum, dan kewenangan menurut hukum.⁷⁵

Pada awalnya yurisdiksi merupakan konsekuensi logis dari kedaulatan negara atas wilayahnya. Yurisdiksi negara atas individu, benda, dan lain-lain dalam batas wilayahnya (teritorial daratan, laut, dan udara). Pada akhirnya dapat berkembang atau meluas melalui batas-batas negara perluasan atas individu dan benda-benda yang tergeletak di negara lain. Yurisdiksi suatu negara tidak terkait hanya tentang ketentuan hukum nasional suatu negara, tetapi juga terkait dengan hukum internasional yang berlaku. Menurut hukum internasional, yurisdiksi diartikan *the*

⁷⁵ Wagiman dan Anasthasya Saartje Mandagi, 2016, Terminologi Hukum Internasional, Sinagrafika, Jakarta Timur, hlm. 494.

*capacity of state under international law to prescribe and enforce a rule of law.*⁷⁶

Yurisdiksi secara sederhana dapat dipahami sebagai suatu kekuasaan negara untuk membuat hukum, menerapkan, dan menegakkan hukum yang dibuatnya. Dalam kerangka pendekatan hubungan antara kekuasaan dan hukum, dapat dikatakan sumber yurisdiksi adalah kedaulatan negara (*state sovereignty*). Kedaulatan negara dalam pengertian modern bukanlah pemahaman kedaulatan produk abad pertengahan yang dipahami sebagai kekuasaan tertinggi (*summa potestas*) yang bersifat mutlak, tidak terbatas, namun dalam pengertian modern ini kedaulatan merupakan kekuasaan tertinggi yang terbatas, dibatasi oleh hukum internasional baik yang berupa perjanjian maupun kebiasaan internasional.⁷⁷

Seperti diketahui, dalam suatu negara berdasarkan teori *trias politica* dari Montesquieu, kedaulatan atau kekuasaan tertinggi suatu negara dalam pelaksanaannya dilaksanakan oleh tiga kategori/ rumpun kekuasaan, yakni: kekuasaan legislatif (*the legislative power*); kekuasaan eksekutif (*the executive power*); dan

⁷⁶ *Ibid.*

⁷⁷ I Made Pasek Diantha, 2020, Hukum Pidana Transnasional, Kencana, Jakarta, hlm. 91.

kekuasaan yudisial (*the judiciary power*). dari ketiga bidang kekuasaan itu muncul tiga jenis yurisdiksi, yakni:⁷⁸

- a. Yurisdiksi perskriptif (*prescriptive jurisdiction*) adalah kekuasaan untuk membuat atau menetapkan aturan hukum.
- b. Yurisdiksi penerapan aturan hukum dan paksaan (*enforcement jurisdiction*) adalah yurisdiksi aparat eksekutif untuk menerapkan dengan paksa aturan hukum baik yang berupa putusan pengadilan maupun yang berupa peraturan perundang-undangan.
- c. Yurisdiksi untuk mengadili (*adjudicative jurisdiction*) adalah yurisdiksi untuk menilai dan memutus dengan adil apakah seseorang telah melanggar hukum atau tidak, baik pelanggaran atas hukum pidana, perdata, maupun administratif.

Menurut I Wayan parthianan, dalam bukunya hukum pidana internasional, pengertian dari ketiganya adalah sebagai berikut.⁷⁹

a. Yurisdiksi Legislatif

Yurisdiksi legislatif merupakan yurisdiksi untuk membuat peraturan perundang-undangan nasional untuk objek hukum yang ada atau terjadi baik didalam dan/atau di luar batas wilayahnya. Yurisdiksi legislatif timbul apabila negara

⁷⁸ *Ibid.*, hlm. 93-94.

⁷⁹ Johannes Irawan, 2018, Pelaksanaan Yurisdiksi Universal Dalam Kedaulatan Nasional Negara-Negara, PT. Rajagrafindo Persada, Depok, hlm. 12.

menghadapi suatu objek hukum yang ternyata belum ada aturan hukum nasional negara yang bersangkutan.

b. Yurisdiksi Eksekutif

Yurisdiksi eksekutif merupakan yurisdiksi suatu negara untuk melaksanakan dan menerapkan hukum atau peraturan perundang-undangan nasionalnya atas suatu objek hukum yang ada atau terjadi di dalam dan/atau di luar batas wilayahnya.

c. Yurisdiksi Yudikatif

Yurisdiksi yudikatif merupakan yurisdiksi suatu negara untuk mengadili dalam artian memaksakan penerapan hukum terhadap pihak yang melakukan peristiwa hukum tersebut yang merupakan pelanggaran hukum atau perundangan nasionalnya.

2. Prinsip-Prinsip Yurisdiksi Secara Umum

Praktik pelaksanaan yurisdiksi di negara-negara di dunia mempunyai :

a. Yurisdiksi Pidana⁸⁰

Yurisdiksi pidana adalah kekuasaan negara untuk membentuk dan menerapkan aturan hukum pidana nasionalnya serta kekuasaan untuk mengadili pelanggarannya. Dalam kerangka studi hukum pidana transnasional, yurisdiksi pidana memiliki peranan penting yakni sebagai landasan keabsahan

⁸⁰ | Made Pasek Diantha, *Op.cit.*, hlm. 96.

bertindak negara dalam menegakkan hukum pidana nasionalnya terkait kejahatan lintas batas negara. mengingat pentingnya peranan yurisdiksi pidana dalam konteks pembahasan hukum pidana transnasional.

b. Yurisdiksi Teritorial⁸¹

Yurisdiksi teritorial adalah yurisdiksi pidana berdasarkan prinsip kewilayahan negara. dalam teknis pelaksanaannya yurisdiksi pidana teritorial dibagi lagi menjadi dua jenis, yakni:

- 1) yurisdiksi pidana teritorial subjektif (*subjective territorial jurisdiction*); dan
- 2) yurisdiksi pidana teritorial objektif (*objective territorial jurisdiction*).

Yurisdiksi pidana teritorial subjektif adalah yurisdiksi pengadilan pidana untuk mengadili pelaku tindak pidana yang tindak pidananya dimulai di dalam wilayah negara dan diselesaikan di wilayah negara lain, *-started in this territory-ended in another state's territory*. Sementara, yurisdiksi pidana teritorial objektif adalah sebaliknya yakni tindak pidana dimulai di wilayah negara lain tetapi diselesaikan di wilayah negara itu sendiri,.... *crime started in another state but... finalised in its own state*.

⁸¹ *Ibid.*, hlm. 97-98.

kecuali terhadap kejahatan internasional (*most serious crime*) yurisdiksi pidana teritorial tidak berlaku terhadap pihak-pihak yang memiliki kekebalan (*imunitas*) yang diakui oleh hukum internasional. Secara garis besar, pihak yang dimaksud antara lain:

- a) pejabat diplomatik sesuai tingkatan;
- b) Pejabat konsuler sesuai tingkatan;
- c) Pejabat organisasi internasional publik, seperti PBB dan uni eropa;
- d) Anggota angkatan bersenjata negara lain;
- e) Hakim-hakim internasional;
- f) Pejabat negara (karena jabatannya) seperti kepala negara, kepala pemerintahan, dan menteri luar negeri;
- g) Misi khusus dari organisasi internasional publik;
- h) Misi khusus dari suatu negara.

Berkenan dengan keberlakuan terhadap yurisdiksi pidana, para pihak tersebut di atas memiliki dua jenis imunitas personal (*personal immunity*) dan imunitas personal (*personal immunity*). Pembagian imunitas seperti itu berkaitan dengan berakhirnya masa berlaku dari imunitas itu. Imunitas fungsional yang dimiliki oleh kepala negara (*head of state*), kepala pemerintahan (*prime minister*) dan menteri luar negeri (*foreign minister*) tidaklah berakhir ketika mereka telah selesai

melaksanakan fungsi dan tugas negaranya di negara asing. Namun imunitas personal semisal dimiliki oleh pejabat diplomatik dan konsuler, imunitasnya akan berakhir setelah tugas misi berakhir, atau *...functional immunity does not cease with the cessation of the function,... in contrast personal privileges and immunities terminate with the cessation of the mission.*

c. Yurisdiksi Personalitas

Yurisdiksi personalitas sering juga disebut yurisdiksi nasionalitas (*nationality jurisdiction*) adalah yurisdiksi yang didasarkan pada prinsip kewarganegaraan. Berdasarkan prinsip itu, yurisdiksi nasionalitas dapat dibedakan menjadi yurisdiksi nasionalitas aktif (*active nationality jurisdiction*) dan yurisdiksi nasionalitas pasif (*passive nationality jurisdiction*).

Dalam konteks hukum pidana transnasional, yurisdiksi nasionalitas aktif berarti kekuasaan negara untuk mengadili warga negaranya yang melakukan kejahatan transnasional di luar negeri,... *adjudicate with respect to conduct of their nationals abroad.* Sementara yurisdiksi nasional pasif berarti kekuasaan negara untuk mengadili pelaku kejahatan transnasional yang korbannya adalah warga negara sendiri,... *to exercise criminal jurisdiction over a person with commit an offence abroad against a national of the state.*

Berkenaan dengan yurisdiksi nasionalitas pasif secara tradisi negara-negara dengan sistem hukum “*common law*” pada umumnya menolak penggunaan yurisdiksi tersebut dengan alasan seperti berikut:⁸²

- 1) Dapat menimbulkan yurisdiksi secara bersamaan (yurisdiksi konkurensi) yang saling tumpang-tindih, karena negara di tempat terjadinya kejahatan juga mempunyai yurisdiksi teritorial terhadap pelaku kejahatan,... *because inevitably resulted in concurent jurisdiction...*
- 2) Dapat menimbulkan ketidakpastian mengenai keleluasaan daya berlakunya, atau *rejected passive personality because of its breadth of indeterminacy*, terutama dalam hal terjadinya yurisdiksi konkurensi (*concurent jurisdiction*).
- 3) Juga dapat menimbulkan permasalahan dasar hukum yang akan dipakai menghukum pelaku kejahatan, misalnya ada kemungkinan di negara asal warga negara itu merupakan tindak pidana, sedangkan di negara tempat terjadinya kejahatan bukan merupakan tindak pidana, atau... *raises issue of legality, particularly of the conduct is an offence in the victim state, but not on the state where it occurs.*

Dalam perkembangannya, negara yang menganut sistem hukum “*common law*” tampaknya telah mengalami

⁸² *Ibid.*, hlm. 98-99.

pengeseran sikap terhadap penerapan yurisdiksi nasionalitas pasif. Pergeseran sikap itu ditunjukkan oleh negara terbesar penganut sistem hukum "*common law*" yakni amerika serikat. Negara ini menerapkan yurisdiksi nasionalitas pasif disebabkan warga negaranya kerap mengalami ancaman/ korban terorisme ataupun penyanderaan di luar negeri,... *it national have repeatedly come under attack while abroad because of their nationality.*

Terkait dengan kejahatan transnasional, dewasa ini dapat dikatakan bahwa hampir semua negara di dunia, baik yang menganut sistem hukum "*common law*" maupun "*civil law*" mengakui eksistensi yurisdiksi nasionalitas pasif, paling tidak oleh semua negara peserta konvensi internasional yang diadakan oleh PBB. Sebagai contoh dapat dilihat ketentuan pasal 15 angka (2) huruf (a) UNTOC yang pada intinya menyatakan bahwa yurisdiksi nasional pasif dapat diterapkan pada kejahatan di luar negeri yang korbannya adalah warga negara sendiri atau,... *subject to article 4 of this convention, a state party may also establish it jurisdiction over any such offence when the offence is committed againts a national of that state party.* Ketentuan serupa juga terdapat dalam pasal 42 angka (2) huruf (a) konvensi PBB melawan korupsi (*UNCAC/ united nations convention against corruption 2003*).

d. Yurisdiksi Kriminal Berdasarkan Prinsip Perlindungan⁸³

Yurisdiksi ini menitikberatkan kepada kepentingan yang harus dilindungi, yakni kepentingan dari negara itu sendiri sebagai suatu pribadi atau subjek hukum dari perbuatan-perbuatan atau kejahatan yang dilakukan oleh masing-masing warga negara lain. Contoh yang sering dikemukakan dalam yurisdiksi ini, misalnya bila kejahatan itu dilakukan di dalam wilayah negara lain yang ditujukan terhadap keamanan, ketertiban, dan kedamaian negara tersebut atau ditujukan kepada instalasi vital milik negara yang bersangkutan. Fokus perlindungan dari yurisdiksi ini adalah kepentingan negara sebagai pribadi hukum dari kejahatan yang dilakukan oleh orang asing dari suatu tempat di wilayah lain.

e. Yurisdiksi Kriminal Berdasarkan Prinsip Universal⁸⁴

Dalam prinsip ini setiap warga negara mempunyai yurisdiksi terhadap tindak kejahatan yang mengancam masyarakat internasional. Yurisdiksi ini lahir tanpa melihat di mana kejahatan itu terjadi atau warga negara yang melakukan kejahatan. Prinsip yurisdiksi universal lahir dikarenakan tidak adanya badan peradilan yang khusus mengadili orang perorangan. Kejahatan yang telah diterima sebagai kejahatan yang tunduk kepada yurisdiksi universal adalah pembajakan

⁸³ Johannes Irawan, *Op.cit.*, hlm. 17.

⁸⁴ *Ibid.*, hlm. 17-18.

dan kejahatan perang. Pembajakan sebagaimana telah ditegaskan di dalam pasal 100 konvensi hukum laut 1982 menyatakan bahwa *“all state shall co-operate to the fullest possible extent in the repression of piracy on the high seas or in any other place outside the jurisdiction of any state.”*

Kejahatan perang juga telah diterima sebagai tunduk kepada yurisdiksi universal di mana setiap negara-negara yang merdeka memiliki hak untuk menghukum kejahatan perang yang tidak terbatas kepada negara, yang warga negaranya menjadi korban ataupun wilayah terjadinya kejahatan tersebut.

F. Tinjauan Umum Mengenai Asas

1. Pengertian Asas

Asas hukum adalah suatu aturan dasar dan prinsip-prinsip hukum yang abstrak dan pada umumnya melatarbelakangi peraturan konkret dan pelaksanaan hukum. Beberapa sarjana memberikan definisi atau pengertian dari asas hukum sebagai berikut:⁸⁵

- a. P.sholten. berpandangan asas hukum adalah kecenderungan-kecenderungan yang di syaratkan oleh pandangan kesusilaan kita pada hukum dan merupakan sifat-sifat umum dengan keterbatasannya sebagai pembawaan yang umum itu, tetapi harus ada.

⁸⁵ Zaeni asyhadie dan arief rahman, 2018, pengantar ilmu hukum, depok, rajawali, hlm.137-138.

- b. Bellefroid menyatakan asas hukum adalah norma dasar yang dijabarkan dari hukum positif dan yang oleh ilmu hukum tidak dianggap berasal dari aturan-aturan yang lebih umum asas hukum umum merupakan pengendapan dari hukum positif.
- c. Eikema hommes mendefinisikan asas hukum bukanlah norma-norma hukum konkret, tetapi ia adalah landasan yang kuat dan paling luas bagi lahirnya peraturan hukum yang berlaku, asas hukum adalah dasar-dasar atau petunjuk arah dalam pembentukan hukum positif.
- d. Sajipto rahardjo menyatakan bahwa asas hukum adalah unsur yang penting dan pokok dari peraturan hukum, asas hukum adalah jantungnya peraturan hukum karena ia merupakan landasan yang paling luas bagi lahirnya peraturan hukum.
- e. Karl larens mengemukakan asas hukum adalah gagasan yang membimbing daalam pengaturan hukum yang mungkin ada atau sudah ada yang dirinya sendiri bukan merupakan aturan yang dapat diterapkan tetapi yang dapat diubah menjadi demikian.⁸⁶
- f. Sudikno mertokusumo menganggap bahwa asas hukum atau prinsip hukum bukanlah peraturan hukum konkret, melainkan merupakan pikiran dasar yang umum sifatnya atau merupakan latar belakang dari peraturan yang konkret yang terdapat dalam dan dibelakang sistem hukum yang terjelma dalam peraturan perundang-undangan dan putusan hakim yang merupakan hukum positif dan dapat diketemukan dengan mencari sifat-sifat umum dalam peraturan konkret tersebut.

Mengenai pandangan dari sajipto raharjo bahwa hukum merupakan unsur penting dan pokok dari peraturan hukum maka dapat di katakan bahwa asas hukum itu merupakan jantungnya peraturan hukum dapat dikatakan dengan dua alasan yaitu: pertama bahwa asas merupakan landasan paling

⁸⁶ Damang dan Apriyanto nusa, 2017, asas dan dasar-dasar ilmu hukum, genta press, yogyakarta, hlm. 55.

luas bagi lahirnya suatu peraturan hukum ini berarti bahwa peraturan-peraturan hukum itu pada akhirnya bisa dikembalikan kepada asas-asas tersebut. Kedua bahwa asas hukum ini layak disebut sebagai suatu sarana bagi lahirnya peraturan hukum atau merupakan peraturan *ratio legis* dari peraturan hukum, asas hukum tidak akan habis kekuatannya dengan melahirkan suatu peraturan hukum selanjutnya.⁸⁷

G. Tinjauan Umum Mengenai Norma

1. Pengertian Dan Jenis-Jenis Norma

Norm dalam bahasa Inggris berasal dari kata *norma* dalam bahasa Latin yang berarti suatu ketertiban, preskripsi atau perintah (Kelsen, 2011:1). Menurut Farrel norma adalah pedoman untuk berperilaku dan dalam pandangan Hage membagi norma menjadi sembilan jenis sebagai berikut:⁸⁸

- a. Norma umum misalnya “dilarang mencuri” atau “setiap” orang yang telah berusia 17 tahun harus memiliki kartu tanda penduduk.
- b. Norma khusus, misalnya bejo harus membayar dua juta kepada doni.

⁸⁷ Said Sambara, 2009, buku ajar pengantar ilmu hukum total media, Yogyakarta, hlm. 81.

⁸⁸ A'an Efendi dan Dyah Ochtorina, 2022, logika dan argumentasi hukum, Kencana, Jakarta, hlm. 75-76.

- c. Norma yang menetapkan hak, contohnya konsumen memiliki hak dari produsen untuk mendapatkan informasi mengenai barang atau jasa yang di belinya.
- d. Norma yang diperbolehkan contohnya silahkan merokok di ruangan yang telah disediakan.
- e. Aturan prosedural mengenai pendirian persoran terbatas harus dengan akta notaris.
- f. Norma perintah contohnya matikan lampu pada saat meniggalkan ruangan.
- g. Petunjuk teknis misalnya minum obat 3 kali sehari pagi, siang , malam.
- h. Norma yang memberi kekuasaan, contohnya kepala daerah berwenang membuat peraturan kepala daerah.
- i. Deskripsi keadaan normatif misalnya di indonesia seorang pengemudi harus mengemudi di sisi kiri jalan.

Menurut asshiddiqe suatu norma dapat berisi sebagai berikut:⁸⁹

- a. Kebolehan atau yang dalam bahasa arab disebut *ibahah mubah* (permittere);
- b. Anjuran postif untuk mengerjakan sesuatu atau dalam hasa arab disebut sunnah;

⁸⁹ *Ibid.*,

- c. Anjuran negatif untuk tidak mengerjakan sesuatu atau dalam bahasa arab disebut makruh;
- d. Perintah positif untuk melakukan sesuatu kewajiban (obligatere) dan
- e. Perintah negatif untuk tidak melakukan sesuatu yang dalam bahasa arab disebut haram atau larangan (prohibere).

Dalam pandangan yang berbeda ruang lingkup sistem norma yang berlaku bagi manusia terbagi sekurang-kurangnya terbagi atas 4 unsur norma, yakni norma moral, norma agama, norma etika (norma sopan santun) dan norma hukum. Keempat norma ini berjalan secara sistematis, simultan dan komplementer bagi manusia dapat diartikan saling bertautan, berketerikatan dan saling melengkapi antara satu dan yang lainnya. Akan penulis jabarkan dengan seperti berikut:⁹⁰

- a. norma moral adalah sebuah sistem aturan yang berlaku bagi manusia yang bersumber dari setiap hati manusia atau sering disebut juga dengan hati nurani yang bekerja atas dasar kesadaran setiap manusia terhadap sekelilingnya (consciousness), dapat diartikan bahwa setiap manusia dikaruniai Tuhan yang maha esa sebuah organ yang mampu menjadi neraca pertimbangan yang setiap saat memberi

⁹⁰ Ilhami bisri, 2004, sistem hukum indonesia prinsip-prinsip dan implementasi hukum di indonesia, raja grafindo persada, depok, hlm.1-5.

pertimbangan atas apa yang di perbuatnya. Jika seorang manusia berbuat salah akan timbul rasas bersalah dan penyesalan yang mendalam maka dari itu semakin sehat hati manusia akan semakin efektif kehidupannya karena senantiasa memperoleh dan mendapatkan pertimbangan hati nurani yang sehat pula.

- b. norma agama adalah sistem aturan yang diperoleh manusia berdasarkan ajaran agama yang dianutnya dapat dikatakan bahwa sumber agama berasal dari ajaran tentang Tuhan yang diperoleh atau yang di turunkan dan disebarluaskan melalui para nabi dan rasul. Alat pengontrol sistem norma agama adalah janji serta sanksi Tuhan yang maha esa berupa pahala bagi manusia yang melaksanakannya dan dosabagi manusia yang inkar terhadap ajaran agamanya.
- c. Norma etika atau norma sopan santun adalah sistem aturan hidup manusia yang berasal dari kesepakatan atau konsensus yang diciptakan oleh dan suatu komunitas masyarakat pada suatu wilayah tertentu. Ukuran norma etika pada dasarnya berupa kepatutan, kepantasan, dan kelayakan yang tumbuh dimasyarakat atau komunitas manusia tersebut. Dapat dikatakan bila terjadi suatu pelanggaran etika maka masyarakat yang akan memberikan reaksi berupa tindakan secara hukuman.

d. Norma hukum adalah sistem aturan yang diciptakan oleh lembaga kenegaraan yang ditunjuk melalui mekanisme tertentu. Artinya hukum diciptakan dan diberlakukan oleh institusi yang memang memiliki kompetensi atau kewenangan dalam membentuk undang-undang yaitu badan legislatif. Norma hukum membuat sanksi yang tegas dan akan segera di jatuhkan apabila dilanggar. Sanksi atau ancaman hukuman yang dijatuhkan bisa berupa paksaan badan atau penjara yang bervariasi sejak dari hukuman kurungan, penjara sampai dengan hukuman mati, atau berupa denda dan sitaan atas benda yang berkaitan dengan pelanggaran yang dilakukan. Seperti halnya norma etika bekerja secara heteronom karena palaksanaan dan penegakkannya dilakukan oleh interaksi antar manusia yang ada pada suatu negara, baik dalam kapasitas sebagai penegak hukum atau sebagai penyelenggara negara yang lain.

Norma-norma hukum alam, seperti norma moralitas yang didedukasi dari norma dasar berdasarkan muatannya sebagai pengeluaran kehendak Tuhan, alam, atau akal budi yang murni dan dianggap sangat jelas. Namun norma dasar sebuah hukum positif hanyalah aturan dasar yang menciptakan norma-norma sistem hukum tersebut, norma tersebut hanya menempatkan fakta material dasar penciptaan hukum. norma dasar ini merupakan

sebuah permulaan proses memiliki karakter dinamis yang sepenuhnya formal. Norma khusus sistem hukum tidak bisa dideduksi secara logis dari norma dasar, tetapi norma khusus harus diciptakan melalui sebuah tindakan khusus yang mengeluarkan atau menetapkannya menjadi bukan sebuah tindakan intelek tetapi dari kehendak. Dalam *pure theory of law* menggunakan norma dasar sebagai dasar hipotesis dengan mempertimbangkan bahwa norma dasar sah serta sistem hukum yang berdasar padanya juga sah. Norma dasar memberi pengertian keharusan pada tindakan pembuat undang-undang pertama pengertian khusus menggabungkan kondisi hukum dengan konsekuensi hukum dalam norma hukum direkonstruksi menjadi bentuk pragmatik yang harus tepat menggambarkan semua data hukum positif. Akhirnya yang berakar pada norma dasar yang memiliki makna normatif yang semua fakta material yang menyusun sistem hukum.

H. Tinjauan Umum Mengenai Jenis-Jenis Ilmu Dan Metode Penafsiran Hukum

1. Jenis-Jenis ilmu penafsiran

Menimbang bahwa masih adanya beberapa rumusan kaidah hukum yang terkandung dalam undang-undang yang secara substansi masih perlu diperjelas atau dilengkapi, maka dari sering terjadinya interpretatif atau multi tafsir dari kaidah kaidah

hukum yang ada, yang berujung pada terjadinya kesalahan dalam mengartikan/ memahami rumusan kaidah hukum yang terkandung dalam undang-undang. Maka dari itu perlu adanya suatu penafsiran hukum yang jelas dan tersistematis agar tidak terjadinya penyimpangan dari pemahaman yang dimaksud oleh pembuat undang-undang. Dengan dilakukannya penafsiran hukum dapat terwujudnya penemuan atau pembentukan kaidah-kaidah hukum yang baru serta terjaminnya kepastian hukum bagi warga negara. selanjutnya penulis akan menuliskan beberapa macam ilmu penafsiran yang akan membantu hakim dan para ahli hukum untuk menerjemahkan hukum seperti berikut:⁹¹

a. Ilmu bahasa

Dalam ilmu bahasa modern telah dikembangkan bahwa salah satu ilmu berkenaan dengan tanda-tanda baca yang populer dikenal dengan istilah semiotik yang diartikan dengan ilmu tentang tanda-tanda baca. Istilah semiotik diperkenalkan oleh John Locke dan dikembangkan sebagai ilmu oleh Charles S Peirce. Semiotik sebagai sebuah disiplin ilmu mempunyai ruang lingkup sangat luas yang termasuk didalamnya seperti ilmu tentang tanda bahasa yakni linguistik yang didalamnya termasuk filologi dan ilmu tentang tanda-tanda lain. Semiotik dapat dibagi menjadi formal semiotik yang didalamnya

⁹¹ Universitas Galuh, Cecep Cahya Supena, "Manfaat Penafsiran Hukum dalam Rangka Penemuan Hukum", [jurnal moderat](#), 31 Mei 2022, hlm.427.

termasuk *cybernetik* dan pengajaran bahasa, serta linguistik murni yang didalamnya terdiri dari cabang linguistik deskriptif, linguistik historika dan perbandingan linguistik, pembagian ini berdasarkan spesialisasi atau keahlian adapula pembagian secara meteril semiotik yang membagi berdasarkan aspek-aspek dari tanda-tanda baca itu sendiri. Dalam buku yang berjudul *sign, language and behavior* yang dikemukakan oleh Ch Morris membagi meteril semiotik menjadi tiga yaitu:⁹²

- 1) Sintatik adalah perkaitan antara tanda-tanda satu dengan tanda-tanda lainnya yang berguna untu memperhatikan bentuk atau struktur tanda-tanda itu.
- 2) Semantik atau juga biasa disebut teori tentang arti-arti yang digunakan untuk mengetahui antara tanda-tanda dan yang diartikan dengan memperhatikan isi tanda-tanda baca itu.
- 3) Pragmatik adalah mempelajari hubungan antara tanda-tanda baca dan pemakainya, digunakann terhadap fungsi tanda-tanda baca

b. Semantik hukum

Secara etimologis semantik berasal dari bahasa inggris yakni *semantics* dan dari segi keilmuan disebut *semasiology* yang berarti suatu ilmu pengetahuan yang menyelidiki makna atau arti kata-kata pada umumnya, dan arti kata-kata dalam

⁹² Nurul Qamar, Dkk. 2017, bahasa hukum (legal language), mitra wacana media, jakarta, hlm.17-19.

berbagai bahasa tertentu dan perhubungannya antara arti dan perubahan arti kata-kata dari zaman ke zaman. Maka bila dihubungkan dengan hukum dapat diartikan bahwa semantik hukum adalah ilmu pengetahuan hukum yang menyelidiki makna atau arti kata-kata hukum, perhubungan dan perubahan arti kata-kata itu dari zaman ke zaman menurut waktu, tempat dan keadaan. Prof hilman memberi contoh tentang semantik dengan menghubungkan arti kata-kata dan perubahannya berdasarkan pergeseran zaman, maka lain halnya dengan Bruggink, yang mencoba membahas tentang semantik dengan menitikberatkan pada aspek pengertian dari arti itu sendiri. Bruggink mengatakan bahwa di dalam semantik ihwalnya adalah berkenaan dengan relasi antara tanda dan yang diartikan. Dalam pembahasan mengenai arti adanya hubungan antara pikiran dan bahasa bahwa apakah arti merupakan sesuatu dari bahasa sehingga arti merupakan suatu sifat atau ciri unsur dari suatu tanda bahasa atau arti merupakan sesuatu yang berasal dari pikiran kita sendiri dalam pembahasan mengenai arti terdapat dua pandangan.

Pandangan pertama mengemukakan bahwa arti adalah suatu sifat dari tanda bahasa artinya sifat dari perkataan dan atau kalimat, penganut pandangan ini memandang bahwa jika arti merupakan sifat dari tanda bahasa maka dapat dikatakan

bahwa harus terdapat hubungan langsung antara tanda dengan yang diartikan, maka dari itu suatu perkataan mempunyai hubungan langsung dengan objek yang dengan perkataan itu mendapatkan suatu nama. Pandangan kedua menolak adanya menolak adanya hubungan langsung antara pernyataan bahasa atau perkataan dengan sesuatu yang dikatakan, pandangan ini berpendirian bahwa suatu pernyataan atau perkataan memperoleh isinya dalam dunia pikiran dari orang yang berbicara. Sesuatu itulah disebut orang pengertian atau *hetbegrip* dengan kata lain konsep dari objek itu, yang juga disebutnya suatu sesuatu isi pikiran. Pandangan ini menganut bahwa arti bukanlah sifat dari perkataan atau kalimat, melainkan pengertian yang diberikan perkataan atau pada satuan bahasa yang lebih luas dari proposisi yang mewujudkan isi dari kalimat.

c. Ilmu Hermeneutika

Pendekatan secara terminologi bersumber dari bahasa Yunani asal kata kerja *hermeneuein* berarti menafsirkan dan dari kata benda *hermeneia* dimaknai sebagai interpretasi. Pemaknaan secara etimologi kata hermeneutika atau hermeneutik merupakan padanan dari bahasa Inggris *hermeneutic* yang diartikan oleh Jazim Hamidi sebagai suatu kata sifat yang berarti ketafsiran. Terdapat tiga kata dari dasar

makna dalam pemakaian aslinya sebagaimana dimaksudkan adalah pertama *hermeneuo* artinya mengungkapkan pikiran-pikiran seseorang dalam bentuk kata-kata. Kedua hermeneuen dimaknai sebagai mengartikan, menerjemahkan dan mengartikan dan ketiga dimaknai sebagai subjek penafsir dan atau yang bertindak sebagai penafsir. Dalam khazanah kefilosafatan ilmu hermeneutik akan masuk dalam ranah filsafat hukum yang mempertanyakan tentang apa yang dikandung hukum itu, bagaimana kandungan hukum itu dan bagaimana hakekat hukum yang sesungguhnya, maka akan melahirkan jawaban yang memberikan arti dan jawaban tentang hukum. Hermeneutik dihubungkan dengan penemuan hukum yang biasa disebut *rechtsvinding* atau *lawfinding* oleh karena itu dengan mengerti dan memahami dapat dilakukan interpretasi dan dari interpretasi dapat dilakukan pencarian untuk menemukan hukum yang tepat untuk di implementasikan dalam suatu kasus-kasus hukum konkret.⁹³

2. Jenis-Jenis Metode Penafsiran

Dalam menjelajahi penafsiran hukum dapat dimulai dengan pendekatan penafsiran yang berfokus kepada teks undang-undang itu sendiri hingga pendekatan kontekstualitas yang memperhitungkan konteks sosial dan tujuan undang-

⁹³ *Ibid.*, hlm.95-100.

undang serta pendekatan sejarah yang melibatkan pemahaman evolusi hukum. Melihat dari sudut pandang bagaimana niat asli pembuat undang-undang dan pendekatan fungsionalitas untuk mencapai hasil yang adil dalam penafsiran hukum berikut beberapa jenis metode penafsiran yang dapat digunakan dalam membantu penafsiran hukum.

a. Penafsiran sistematis

Penafsiran sistematis yang disebut juga penafsiran dogmatis adalah penafsiran yang bermaksud untuk menghubungkan bunyi pasal-pasal dari suatu peraturan dengan peraturan lainnya, sehingga suatu peraturan itu anmpak hubungan antara satu dengan yang lainnya.⁹⁴

b. Penafsiran sejarah atau historis

Penafsiran ini melihat dari dua segi yaitu pertama melihat dari sejarah hukumnya yaitu penafsiran yang bermaksud menyelidiki asal-usul terbentuknya suatu peraturan hukum dari dahulu sampai sekarang contohnya: *code civil* perancis yang ada pengaruhnya dalam undang-undang perdata belanda seterusnya dalam KUHPerdata indonesia. Kedua melihat sejarah undang-undang yaitu penafsiran yang

⁹⁴ Said sampara, *Op.Cit.*, hlm.178.

bermaksud menyelidiki apa maksud pembuat undang-undang didalam menetapkan suatu undang-undang.⁹⁵

c. Penafsiran sosiologis (teleologis)

Penafsiran teleologis yang disebut juga penafsiran sosiologis adalah penafsiran undang-undang sedemikian rupa sehingga undang-undang itu dapat dijalankan serasi dengan keadaan masyarakat. Jadi penafsiran ini sebenarnya bermaksud untuk mencari makna undang-undang buat keadaan sekarang, untuk mencapai tujuan yang terkandung dalam undang-undang yang bersangkutan paut dengan kebutuhan masyarakat. Contohnya terjadi pada zaman pemerintahan hindia belanda dahulu yang sekarang masih tetap berlaku sudah barang tentu banyak yang tidak sesuai lagi dengan keadaan sekarang sehingga untuk menyesuaikan dengan keadaan sekarang undang-undang itu perlu ditafsirkan secara teleologis dari kata telos yang berarti tujuan atau secara sosiologis yang berarti sesuai dengan keadaan.⁹⁶

d. Penafsiran otentik (offisil)

Penafsiran otentik disebut juga penafsiran offisil yang berarti penafsiran yang dikemukakan, dicantumkan dalam bentuk penjelasan atau khusus dalam pasal undang-undang, sebagai tafsiran resmi oleh pembuat undang-undang, tafsiran

⁹⁵ *Ibid.*, hlm.178-179.

⁹⁶ *Ibid.*, hlm.179.

ini diadakan oleh pembuat undang-undang agar dapat diikuti oleh pihak-pihak yang berkompeten dan berkepentingan.⁹⁷

e. Penafsiran gramatikal

Penafsiran gramatikal terkait pada bunyi ketentuan undang-undang dengan berpedoman pada arti perkataan-perkataan dalam hubungannya satu sama lain dalam kalimat-kalimat yang dipakai oleh undang-undang ialah semata-mata arti perkataan menurut tata bahasa atau menurut kebiasaan yakni dalam arti pemakaian sehari-hari.⁹⁸

f. Penafsiran perbandingan

Penafsiran perbandingan ialah suatu penafsiran dengan membandingkan antara hukum lama dengan hukum positif yang berlaku saat ini antara hukum nasional dengan hukum asing dan hukum kolonial. Dalam penafsiran perbandingan akan terlihat antara lain bahwa hukum lama dengan hukum positif yang berlaku saat ini mungkin hukum lama yang cocok untuk diterapkan lagi pada masa sekarang ini. Umpamanya beberapa hukum dan asas hukum adat yang menggambarkan unsur kekeluargaan dapat diambil untuk dijadikan hukum nasional.⁹⁹

⁹⁷ *Ibid.*,

⁹⁸ *Ibid.*, hlm.178.

⁹⁹ R, Soeroso, 2016, pengantar ilmu hukum, sinar grafika offset, jakarta, hlm.108.

I. Tinjauan Umum Mengenai Asas Preferensi Hukum

Asas preferensi hukum adalah asas-asas hukum yang merujuk pada hukum mana yang digunakan atau didahulukan keberlakuannya jika dalam suatu peristiwa hukum terkait atau terlanggar beberapa peraturan. Maka dari itu penyelesain norma yang bertentangan berlaku asas preferensi hukum yang meliputi asas-asas sebagai berikut:¹⁰⁰

- a. *Lex specialis derogat legi generali* artinya hukum yang khusus mencabut hukum yang umum. Menurut purnadi purbacaraka dan soerjono soekanto yang dimaksudkan dari asas ini mengacu terhadap peristiwa yang khusus wajib diberlakukan undang-undang yang menyebut peristiwa itu, walaupun untuk peristiwa khusus tersebut dapat pula diberlakukan undang-undang yang menyebut peristiwa khusus tersebut. Keberlakuan asas ini ditujukan agar tidak munculnya keragu-raguan pada hakim jika terjadi kasus yang diatur dalam dua undang-undang.¹⁰¹ Dalam asas ini apabila terdapat sebuah undang-undang yang mengatur sebuah substansinya yang bersifat umum dan luas ruang lingkupnya berhadapan dengan undang-undang yang substansinya lebih khusus dan ruang lingkupnya

¹⁰⁰ A'an efendi dan Dyah ochtorina susanti, *Op.Cit.*, hlm.86.

¹⁰¹ Purnadi purbacaraka dan soerjono soekanto, 1983, perundang-undangan dan yurisprudensi, citra aditya bakti, bandung, hlm.8.

lebih sempit maka yang digunakan adalah undang-undang yang substansinya lebih khusus dan sempit tersebut.¹⁰²

- b. *Lex posterior generalis non derogat priori specialis* artinya hukum umum yang berlaku kemudian tidak mencabut hukum khusus yang berlaku terdahulu.
- c. *Lex posterior derogat legi priori* artinya hukum yang kemudian mencabut hukum yang terdahulu. Asas hukum ini digunakan manakala terjadi konflik norma secara horizontal yaitu konflik norma yang terjadi diantara peraturan perundang-undangan yang sederajat yang mengatur substansi yang sama dan sejenis. Diatasi dengan berpedoman pada aspek keberlakuan yuridis peraturan perundang-undangan yang terbaru atau yang sesuai dengan zaman diantara undang-undang yang saling bertentangan tersebut.¹⁰³
- d. *Lex superior derogat legi inferiori* artinya hukum yang memiliki hierarki yang lebih tinggi mengalahkan hukum yang hierarkinya lebih rendah.

¹⁰² Umar anwar, dkk, 2022, pengantar ilmu hukum, yayasan penerbit muhammad zani, aceh, hlm.137.

¹⁰³ *Ibid*,.