

**ANALISIS YURIDIS TERHADAP TINDAK
PIDANA YANG BERAKIBAT TERGANGGUNYA
SISTEM ELEKTRONIK**

(Studi Putusan Nomor 25/Pid.Sus/2019/PN Unh)

SKRIPSI

Diajukan Untuk Memenuhi Tugas Dan Melengkapi
Syarat Memperoleh Gelar Sarjana Program Strata 1 (S.1)



Disusun oleh :

Muhammad Mirza Kurniawan

1902056111

PROGRAM STUDI ILMU HUKUM

FAKULTAS SYA'RIAH DAN HUKUM

UNIVERSITAS ISLAM NEGERI WALISONGO

2024

PERSETUJUAN PEMBIMBING



KEMENTERIAN AGAMA
UNIVERSITAS ISLAM NEGERI WALISONGO
FAKULTAS SYARIAH DAN HUKUM

Jl. Prof Dr. Hamka Kampus III Ngaliyan Telp./Fax. (024) 7601291/7624691 Semarang 50185

PERSETUJUAN PEMBIMBING

Lamp : 4 (Empat) Eks.
Hal : Naskah Skripsi

An. Sdra. Muhammad Mirza Kurniawan

Kepada Yth.
Dekan Fakultas Syariah dan Hukum
UIN Walisongo Semarang Di Semarang
Assalamu 'alaikum Wr. Wb.

Setelah saya melakukan penelitian dan mengadakan perbaikan seperlunya, bersama ini saya kirim naskah skripsi Saudara:

Nama : Muhammad Mirza Kurniawan

NIM : 1902056111

Prodi : Ilmu Hukum

Judul Skripsi : Analisis Yuridis Terhadap Tindak Pidana Yang
Mengakibatkan Terganggunya Sistem Elektronik (Studi
Putusan No. 25/Pid.Sus/2019/PN Unh)

Dengan ini saya mohon sekiranya skripsi saudara tersebut dapat segera di
munaqasyahkan. Demikian, harap menjadi maklum.

Wassalamu 'alaikum Wr. Wb.

Semarang, 14 Juni 2024
Pembimbing II

Pembimbing I

Dr. M. Harun, S.Ag, M.H

NIP: 197508152008011017

Nazar Nurdin M.S.I

NIP: 199002222019031015

PENGESAHAN



KEMENTERIAN AGAMA
UNIVERSITAS ISLAM NEGERI WALISONGO
FAKULTAS SYARIAH DAN HUKUM

Alamat: Jl. Prof. Dr. Hamka Kampus III Ngalyan Telp./Fax. (024) 7601291/7624691 Semarang 50185

PENGESAHAN

Skripsi Saudari : Muhammad Mirza Kurniawan
NIM : 1902056111
Program Studi : Ilmu Hukum
Judul : Analisis Yuridis Terhadap Tindak Pidana yang Mengakibatkan
Terganggunya Sistem Elektronik (Studi Putusan Nomor
25/Pid.Sus/2019/PN Unh)

Telah dimunaqosahkan oleh Dewan Penguji Fakultas Syari'ah dan Hukum UIN Walisongo Semarang dan telah dinyatakan lulus, pada tanggal 25 Juni 2024 dan dapat diterima sebagai syarat guna memperoleh gelar Sarjana Strata 1 (satu) tahun akademik 2023/2024.

Semarang, 10 Juli 2024

Ketua Sidang

AHMAD FUAD AL-ANSHARY, S.H.I., M.S.I.
NIP. 19880916203211027

Sekretaris Sidang

Dr. M. HARUN, S.Ag., M.H.
NIP. 197508152008011017

Penguji Sidang I

AHMAD ZUBAERI, M.H.
NIP. 199005072019031010

Penguji Sidang II

DAUD RISMANA, M.H.
NIP. 199108212019031014

Pembimbing I

Dr. M. HARUN, S.Ag., M.H.
NIP. 197508152008011017

Pembimbing II

Nazar Nurdin, M.S.I.
NIP. 199002222019031015



MOTTO

وَلَا تَأْكُلُوا أَمْوَالَكُمْ بَيْنَكُمْ بِالْبَاطِلِ وَتُدُلُّوا بِهَا إِلَى الْحُكَّامِ لِتَأْكُلُوا فَرِيقًا
مِّنْ أَمْوَالِ النَّاسِ بِالْإِثْمِ وَأَنْتُمْ تَعْلَمُونَ

“Dan janganlah kamu makan harta di antara kamu dengan jalan yang batil, dan (janganlah) kamu menyuap dengan harta itu kepada para hakim, dengan maksud agar kamu dapat memakan sebagian harta orang lain itu dengan jalan dosa, padahal kamu mengetahui” (Q.S Al-Baqarah 2:188)

PERSEMBAHAN

Dengan menyebut Alhamdulillahirabbil`alamin sebagai rasa syukur kepada Allah SWT yang telah memberikan rahmat, ridha, dan pertolongan- Nya kepada penulis sehingga penulis dapat menyelesaikan skripsi dan studi strata satu ini dengan lancar. Pada kesempatan ini dengan segenap rasa terima kasih yang penulis miliki kepada beberapa pihak yang telah membantu dalam proses penyelesaian skripsi ini, maka skripsi ini penulis persembahkan untuk:

1. Kepada Orang tua tercinta penulis, Bapak Moch Sodikin dan Ibu Chusnul Chotimah yang telah memberikan segalanya bagi penulis, terimakasih atas kasih sayang, support, nasehat dan doa yang terus mengalir dengan tulus dan ikhlas untuk kesuksesan anak-anaknya.
2. Bapak Dr. M. Harun, S.Ag. M.H. selaku Pembimbing I dan Bapak Nazar Nurdin, M.S.I selaku Pembimbing II yang selalu memberikan masukan kepada penulis dalam menyelesaikan skripsi ini.
3. Teman-teman terdekat penulis, yang senantiasa memberikan bantuan, doa, semangat, dan menemani penulis.
4. Kepada diri saya sendiri, terima kasih untuk tidak menyerah, tidak berhenti untuk berusaha melakukan yang terbaik, dan masih bertahan hingga saat ini.

PERNYATAAN ORISINALITAS

DEKLARASI

Dengan penuh kejujuran dan tanggungjawab, penulis menyatakan bahwa skripsi yang berjudul "Analisis Yuridis Terhadap Tindak Pidana Yang Mengakibatkan Terganggunya Sistem Elektronik (Studi Putusan Nomor 25/Pid.Sus/2019/Pn Unh)" tidak berisi materi yang pernah ditulis oleh orang lain atau di terbitkan. Demikian juga skripsi ini tidak berisi satupun pikiran orang lain, kecuali informasi yang terdapat dalam referesnsi yang dijadikan bahan rujukan

Semarang, 19 Juni 2024

Deklarator



Muhammad Mirza Kurniawan

NIM 1902056111

PEDOMAN TRANSLITERASI

Pedoman transliterasi yang digunakan adalah Sistem Transliterasi Arab Latin SKB Menteri Agama RI No. 158/1987 dan Menteri Pendidikan dan Kebudayaan No. 0543b/1987 tertanggal 22 Januari 1998.

A. Konsonan Tunggal

Huruf Arab	Nama	Huruf Latin	Keterangan
ا	Alif	-	Tidak dilambangkan
ب	Ba	B	Be
ت	Ta	T	Te
ث	Sa	Ṣ	Es (dengan titik di atas)
ج	Jim	J	Je
ح	Ha	ḥ	Ha (dengan titik di bawah)
خ	Kha	Kh	Ka dan Ha
د	Dal	D	De
ذ	Dzal	Dz	De dan Zet
ر	Ra	R	Er
ز	Zai	Z	Zet
س	Sin	S	Es
ش	Syin	Sy	Es dan Ye
ص	Sad	Ṣ	Es (dengan titik di bawah)
ض	Dad	Ḍ	De (dengan titik di bawah)
ط	Ta	Ṭ	Te (dengan titik di bawah)
ظ	Za	Ẓ	Zet (dengan titik di bawah)
ع	'ain	‘	Koma terbalik (di atas)
غ	Gain	G	Ge
ف	Fa	F	Ef
ق	Qaf	Q	Ke
ك	Kaf	K	Ka
ل	Lam	L	El
م	Mim	M	Em

ن	Nun	N	En
و	Wawu	W	We
هـ	Ha	H	Ha
ء	Hamzah	'	Apostrof
ي	Ya	Y	Ye

B. Konsonan Rangkap

Konsonan rangkap (*tasydid*) ditulis rangkap

Contoh: مقدمه ditulis *Muqaddimah*

C. Vokal

1. Vokal Tunggal

Fathah ditulis “a”. Contoh: فتح ditulis *fataḥa*

Kasrah ditulis “i”. Contoh: علم ditulis *‘alimun*

Dammah ditulis “u”. Contoh: كتب ditulis *kutub*

2. Vokal Rangkap

Vokal rangkap (fathah dan ya) ditulis “ai”.

Contoh: اين ditulis *aina*

Vokal rangkap (fathah dan wawu) ditulis “au”.

Contoh: حول ditulis *ḥaula*

D. Vokal Panjang

Fathah ditulis “a”. Contoh: باع = *bā ‘a*

Kasrah ditulis “i”. Contoh: عليهم = *‘alī mun*

Dammah ditulis “u”. Contoh: علوم = *‘ulūmun*

E. Hamzah

Huruf Hamzah (ء) di awal kata tulis dengan vokal tanpa didahului oleh tanda apostrof (‘). Contoh: ايمان = *īmān*

F. Lafzul Jalalah

Lafzul jalalah (kata الله) yang terbentuk frase nomina ditransliterasikan tanpa hamzah. Contoh: عبدالله ditulis *‘Abdullah*

G. Kata Sandang “al-...”

1. Kata sandang “al-” tetap ditulis “al-”, baik pada kata yang dimulai dengan huruf qamariyah maupun syamsiyah.
2. Huruf “a” pada kata sandang “al-” tetap ditulis dengan huruf kecil.
3. Kata sandang “al-” di awal kalimat dan pada kata “Al-Qur’an” ditulis dengan huruf kapital.

H. Ta marbutah (ة)

Bila terletak diakhir kalimat, ditulis h, misalnya: البقرة ditulis *al-baqarah*. Bila di tengah kalimat ditulis t. Contoh: زكاة المال ditulis *zakāh al-māl* atau *zakātul māl*.

ABSTRAK

Teknologi informasi dan komunikasi yang canggih dalam praktiknya memberikan kemudahan bagi siapapun yang mengakses informasi. Namun, kemudahan yang diberikan teknologi membuat sebagian orang menyalahgunakannya. Salah satu perbuatan tersebut dinamakan *defacing* (penyalahgunaan teknologi dengan cara menerobos *website* tanpa izin pemilik *website*). Undang-undang Republik Indonesia Nomo 19 Tahun 2016 Tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik telah mengantisipasi atas pengaruh buruk dari pemanfaatan kemajuan teknologi tersebut. Maka dari itu, penelitian ini bertujuan untuk membahas secara mendalam terkait kasus tindak pidana yang berakibat pada terganggunya sistem elektronik dalam suatu putusan dan menilik bagaimana pertimbangan hakim dalam memutuskan perkara tersebut. Kasus tindak pidana ini terdapat pada Putusan Nomor 25/Pid.Sus/2019/PN Unh. Dalam putusan tersebut seorang pelaku berusia 22 tahun melakukan *defacing* terhadap *website* Pengadilan Negeri Unaaha, Sulawesi Tenggara. Penelitian ini menggunakan jenis penelitian yuridis normatif dan pendekatan perundang-undangan (*statute approach*) dan pendekatan konseptual (*conseptual approach*). Adapun pengumpulan data diambil dengan cara studi kepustakaan (*library research*). Hasil penelitian menunjukkan bahwa perbuatan pelaku terbukti melanggar Undang Undang Informasi dan Transaksi Elektronik karena telah memenuhi unsur setiap orang dan unsur sengaja. Pertimbangan hakim dalam hal ini menggunakan beberapa teori yaitu teori absolut, teori relatif, teori gabungan, dan teori keseimbangan. Dengan memperhatikan berbagai aspek tersebut secara komprehensif, putusan hakim diharapkan dapat mencerminkan keseimbangan antara kepentingan hukum dan rasa keadilan masyarakat.

Kata Kunci: Tindak Pidana, Sistem Elektronik, *Defacing*, Putusan, Pertimbangan Hakim

ABSTRACT

In practice, sophisticated information and communication technology makes it easy for anyone to access information. However, the convenience provided by technology makes some people abuse it. One of these actions is called defacing (misuse of technology by breaking into a website without the permission of the website owner). The Republic of Indonesia Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 on Electronic Information and Transactions has anticipated the negative effects of utilizing these technological advances. Therefore, this research aims to discuss in depth criminal cases that result in disruption of the electronic system in a decision and examine how the judge considers when deciding the case. This criminal case is contained in Decision Number 25/Pid.Sus/2019/PN Unh. In this decision, a 22 year old perpetrator committed defacing on the Unaaha District Court website, Southeast Sulawesi. This research uses a normative juridical research type and a statutory approach (statute approach) and conceptual approaches (conceptual approach). The data collection was taken by means of literature study (library research). The results of the research show that the perpetrator's actions were proven to have violated the ITE Law because they fulfilled the elements of every person and the elements of deliberate action. The judge's considerations in this case used several theories, namely absolute theory, relative theory, combined theory and balance theory. By considering these various aspects comprehensively, the judge's decision is expected to reflect a balance between legal interests and society's sense of justice.

Keywords: Crime, Electronic Systems, Defacing, Decision, Judge's Considerations

KATA PENGANTAR

Assalamualaikum Wr. Wb.

Dengan menyebut nama Allah Yang Maha Pengasih lagi Maha Penyayang. Alhamdulillah, segala puji bagi Allah SWT atas segala rahmat dan kemudahan yang diberikan oleh-Nya sehingga penulis dapat menyelesaikan penelitian tugas akhir (skripsi) dengan lancar dan sesuai dengan yang diharapkan. Sholawat serta salam semoga tetap tercurahkan kepada junjungan kita Nabi Muhammad SAW, keluarga, sahabat, dan seluruh umatnya.

Skripsi ini merupakan wujud karya terakhir yang peneliti susun dalam rangka memenuhi salah satu syarat untuk mencapai derajat Sarjana Strata 1 Program Studi Ilmu Hukum Fakultas Syariah dan Hukum UIN Walisongo Semarang. Dalam proses penyusunan skripsi ini tidak lepas dari berbagai hambatan yang mengganggu dan peneliti memperoleh banyak bantuan serta dukungan dari berbagai pihak, untuk peneliti mengucapkan banyak terimakasih kepada:

1. Bapak Prof. Dr. Nizar, M.Ag. selaku Rektor Universitas Islam Negeri Walisongo beserta jajarannya
2. Bapak Prof. Dr. Abdul Ghofur, M.Ag. selaku Dekan Fakultas Syariah dan Hukum Universitas Islam Negeri Walisongo
3. Ketua Jurusan Ilmu Hukum Ibu Dr. Novita Dewi Masyithoh, S.H, M.H dan Sekretaris Jurusan Ilmu

Hukum Ibu Mahdaniyal Hasanah Nuriyyatiningrum,
M.S.I.

4. Bapak Dr. M. Harun, S.Ag., MH. Selaku Pembimbing I dan Bapak Nazar Nurdin, M.S.I., selaku Pembimbing II yang dengan ikhlas memberikan bimbingan, dukungan semangat, masukan, kritik, dan saran terhadap penelitian skripsi penulis. Kerelaan beliau dalam mengorbankan waktu, tenaga, dan pikiran merupakan salah satu faktor keberhasilan penulis dalam menyelesaikan skripsi ini.
5. Ibu Fithriyatus Sholihah, S.H.I., M.H. selaku Wali Dosen penulis, atas segala kesabaran, dukungan dan arahan baik yang diberikan penulis selama menjalani perkuliahan.
6. Kedua orang tua penulis, bapak Moch Sodikin dan Ibu Chusnul Chotimah yang telah mengasuh mendidik dan dengan tulus, sabar, selalu mendoakan, memberi motivasi. baik materiil maupun/1 non materiil kepada penulis, sehingga penulis mampu menyelesaikan tugas akhir ini.
7. Abah Kyai Zainal Arifin, S.H.I.,M.Ag Al-Hafidz dan Ibu Nyai Ismah, M.Pd selaku pengasuh Pondok Pesantren Al-Qur'an Al Masthuriyah Semarang yang selama ini peneliti dari awal masuk kuliah hingga sekarang menuntut ilmu ngaji di pondok beliau.
8. Santri-santri Pondok Pesantren Al-Qur'an Al Masthuriyah, khususnya kamar 6 yang menjadi tempat bernaung selama penulis dalam menyelesaikan tugas akhir ini.

9. Seluruh teman-teman seperjuangan Ilmu Hukum 2019 yang tidak bisa penulis sebutkan satu-persatu yang telah berjuang bersama penulis untuk menuntut ilmu di Universitas Islam Negeri Walisongo.
10. Seluruh pihak yang membantu, mendoakan, mendukung penulis dalam menyelesaikan skripsi ini yang tidak dapat disebutkan satu-persatu, semoga Allah SWT selalu memberikan limpahan keberkahan kepada kalian semua.

Penulis berharap, semoga skripsi ini dapat memberikan manfaat baik kepada penulis maupun pembaca terkhusus pada bidang Ilmu Hukum. Penulis menyadari bahwa penulisan skripsi ini jauh dari kesempurnaan, oleh karena itu penulis memohon maaf dan mengharapkan masukan, kritik dan saran yang membangun dari para pembaca agar penulis dapat menjadi pembelajaran baru bagi penulis

Semarang, 18 Juni 2024

Penulis



Muhammad Mirza Kurniawan

NIM 1902056111

DAFTAR ISI

PERSETUJUAN PEMBIMBING	i
PENGESAHAN	ii
MOTTO	iii
PERSEMBAHAN	iv
PERNYATAAN ORISINALITAS	v
PEDOMAN TRANSLITERASI	vi
ABSTRAK	ix
ABSTRACT	x
KATA PENGANTAR	xi
DAFTAR ISI	xiv
BAB I PENDAHULUAN	1
A. Latar Belakang	1
B. Rumusan Masalah	14
C. Tujuan Penelitian.....	15
D. Manfaat Penelitian.....	15
E. Telaah Pustaka.....	17
F. Metode Penelitian.....	21
G. Sistematika Penulisan.....	25

BAB II TINJAUAN TEORITIK TENTANG TINDAK PIDANA, KEJAHATAN DUNIA MAYA (CYBER CRIME), SISTEM ELEKTRONIK..... 27

A. Tindak Pidana 27

 1. Pengertian..... 27

 2. Unsur-Unsur 31

 3. Jenis-jenis Tindak Pidana..... 36

B. Kejahatan Dunia Maya (*CyberCrime*) 42

 1. Pengertian..... 42

 2. Jenis-jenis 44

C. Sistem Elektronik..... 50

 1. Pengertian..... 50

 2. Jenis-jenis Sistem Elektronik 52

 3. Ancaman dan Serangan yang Mengakibatkan Terganggunya Sistem Elektronik 55

BAB III PUTUSAN PENGADILAN NEGERI UNAHAA NOMOR 25/PID.SUS/2019/PN UNH TENTANG TINDAK PIDANA YANG BERAKIBAT TERGANGGUNYA SISTEM ELEKTRONIK..... 68

A. Posisi Kasus..... 68

B. Substansi Putusan 70

C. Pertimbangan Hakim..... 86

D. Amar Putusan 91

BAB IV ANALISIS PUTUSAN PENGADILAN NEGERI UNAAHA (NOMOR 25/PID.SUS/2019/PN UNH) TERHADAP TINDAK PIDANA YANG MENAKIBATKAN TERGANGGUNYA SISTEM ELEKTRONIK.....	93
A. Pertimbangan Hukum Hakim Terhadap Tindak Pidana yang Berakibat Terganggunya Sistem Elektronik Pada Putusan Pengadilan Negeri Unaaaha Nomor 25/Pid.Sus/2019/PN UNH.....	93
B. Analisis Yuridis Terhadap Tindak Pidana yang Berakibat Terganggunya Sistem Elektronik Dalam Putusan Pengadilan Negeri Unaaaha Nomor 25/Pid.Sus/2019/PN UNH	103
BAB V PENUTUP	111
A. Simpulan.....	111
B. Saran.....	112
DAFTAR PUSTAKA	1144
LAMPIRAN.....	122
DAFTAR RIWAYAT HIDUP.....	Error! Bookmark not defined.

BAB I

PENDAHULUAN

A. Latar Belakang

Perkembangan teknologi informasi yang terjadi dalam masyarakat saat ini tidak dapat dihindari lagi. Teknologi informasi menjadi salah satu kebutuhan yang penting bagi manusia. Banyak perubahan yang terjadi dalam pemenuhan kebutuhan masyarakat yang pada awalnya bersifat analogi menjadi bersifat serba digital.

Hal tersebut dapat dilihat pada era modern saat ini, dimana teknologi informasi menjadi suatu tren perkembangan teknologi. Teknologi informasi sebagai suatu bidang ilmu yang berkembang sangat cepat saat ini dan memiliki pengaruh yang sangat besar terhadap perkembangan peradaban manusia.

Teknologi saat ini yang bisa memudahkan manusia untuk melakukan apapun seperti belanja lewat *online shop* (toko *online*), memesan makanan atau menyewa jasa lewat aplikasi tertentu, serta juga dapat digunakan untuk sarana diskusi, simulasi, dan kegiatan pembelajaran.¹ Teknologi informasi dan komunikasi dalam praktiknya tidak hanya digunakan sebatas fasilitas untuk berbicara, tetapi juga untuk hiburan. Adanya kebutuhan tersebut, teknologi informasi menghasilkan bermacam aplikasi serta portal- portal hiburan *online*.

Seiring perkembangan teknologi yang semakin pesat saat ini dapat menghubungkan kita yang jauh menjadi dekat serta bisa memudahkan manusia dalam melakukan

¹ Suherman, Ade Maman, *Aspek Hukum Dalam Teknologi*, (Jakarta: Ghalia Indonesia, 2002), 28.

aktivitasnya. Hadirnya teknologi ini membantu manusia dalam beraktivitas baik secara langsung maupun tidak langsung, serta dapat berinteraksi tanpa mengenal batasan ruang dan waktu. Dengan memanfaatkan adanya teknologi, manusia pun berlomba-lomba untuk memunculkan inovasi-inovasi terbaru guna mempermudah kebutuhan hidup dan kesejahteraannya.

Kecanggihan yang dihadirkan oleh teknologi inilah yang nanti tentunya membuat masyarakat mudah dalam mengakses hiburan-hiburan tanpa keluar dari rumah mereka. Namun, kemudahan yang diberikan teknologi membuat sebagian orang menyalahgunakannya. Penyalahgunaan teknologi data bisa berbentuk membuat konten kabar palsu, pelanggaran hak cipta semacam mengunggah video dengan tema ataupun konten tertentu yang sudah mempunyai hak cipta, pencemaran nama baik dalam wujud video, gambar, tulisan yang diterbitkan, serta lain-lain. Teknologi informasi saat ini laksana dua sisi mata uang karena selain memiliki andil dalam peningkatan kesejahteraan, kemajuan, dan peradaban manusia, sekaligus menjadi sarana efektif perlawanan melawan hukum.¹

Banyak aspek yang dipengaruhi oleh teknologi salah satunya kegiatan komunikasi. Internet merupakan salah satu teknologi yang banyak dimanfaatkan oleh masyarakat. Sebagai produk teknologi maka internet dapat melahirkan suatu jenis interaksi sosial yang

¹ Lampiran Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik

berbeda dengan intraksi sosial sebelumnya.² Dengan majunya teknologi informasi dan komunikasi saat ini, terdapat pengaruh baik positif maupun negatif bagi masyarakat. Di satu sisi pemanfaatan teknologi informasi dan komunikasi berkontribusi memberikan peningkatan kesejahteraan dan peradaban manusia, di sisi lain jika digunakan dengan tidak bijak dapat dimanfaatkan untuk melancarkan perbuatan melawan hukum yang dapat menyerang kepentingan siapa saja.³

Namun dibalik kelebihan dan kemudahan yang ditawarkan oleh komputer dan internet, ternyata memiliki sisi gelap yang dapat menghancurkan kehidupan dan budaya manusia itu sendiri. Semakin canggihnya teknologi itu berkembang, akan muncul bentuk-bentuk kejahatan yang terjadi dewasa ini yang semakin variatif, sebab ada suatu media atau saluran baru untuk timbulnya suatu tindak kejahatan.⁴ Selain itu, komputer dan internet sebagai ciptaan manusia memiliki karakteristik mudah dieksploitasi oleh siapa saja yang memiliki keahlian dalam bidang tersebut.

Sehingga, dapat dikatakan perkembangan teknologi informasi saat ini menjadi pedang bermata dua karena selain memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan, dan peradaban manusia, sekaligus menjadi sarana efektif perbuatan melawan

² Shiefti Dyah Alyusi. *Media Sosial: Interaksi, Identitas, dan Modal Sosial*. (Jakarta: Kencana, 2016), 1.

³ Adami Chazawi dan Ferdian Adi, *Tindak Pidana Informasi dan Transaksi Elektronik*, (Malang, Media Nusa Creative, 2015), 2.

⁴ Maskun, *Kejahatan Siber Cyber Crime: Suatu Pengantar*, (Jakarta: Kencana, 2013), 82.

hukum.⁵ Internet dan teknologi informasi merupakan inovasi baru pada dekade terakhir ini dan sangat mempengaruhi kehidupan manusia. Beberapa aktivitas manusia berubah secara signifikan dengan mengambil keuntungan dari efisiensi, efektifitas, dan mobilitas. Sayangnya, kemajuan teknologi ini juga memperkenalkan permasalahan-permasalahan baru saat digunakan secara tidak tepat atau menyalahi dari yang semestinya. *Cybercrime*, itulah sebutan untuk perbuatan melawan hukum dalam dunia maya.

Kejahatan *cyber (cybercrime)* ini adalah bentuk ancaman baru yang belum pernah ada sebelumnya pada masyarakat dunia. *Hacking, cracking, defacing, sniffing, carding, phishing, spamming*, ataupun *scam* merupakan sederet kejahatan internet yang cukup berbahaya dan telah menimbulkan kerugian nyata bagi para korbannya.

Cybercrime menurut Indra Safitri adalah kejahatan dunia maya 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.⁶ Secara singkat, *cybercrime* dapat diartikan dengan istilah yang mengacu kepada aktivitas kejahatan dengan komputer atau jaringan komputer menjadi alat, sasaran atau tempat terjadinya

⁵ Budi Suhariyanto, *Tindak Pidana Teknologi Informasi (Cybercrime) Urgensi dan Pengaturan Celah Hukumnya*, Jakarta: Raja Grafindo Persada, 2012,

⁶ M.Ade Chairuddin Najib, *Sanksi Terhadap Tindak Pidana Defacing Dalam Undang Undang Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik Dengan Prespektif Hukum Islam*, skripsi Universitas Islam Negeri Raden Fatah, Palembang, 2018, 37-38.

kejahatan. Namun ada juga yang berpendapat bahwa kejahatan dunia maya (*cybercrime*) itu adalah tindakan kriminal yang dilakukan dengan menggunakan teknologi komputer sebagai alat kejahatan utama.

Cybercrime merupakan kejahatan yang memanfaatkan perkembangan teknologi komputer khususnya internet. *Cybercrime* didefinisikan sebagai perbuatan melanggar hukum yang memanfaatkan teknologi komputer yang berbasis pada kecanggihan perkembangan teknologi internet. *Cybercrime* merupakan salah satu sisi gelap dari kemajuan teknologi yang mempunyai dampak negatif yang sangat luas bagi seluruh bidang kehidupan modern saat ini⁷

Website sebagai salah satu aplikasi dari internet merupakan media yang juga sangat membantu dalam perkembangan teknologi komunikasi dalam masa kini. *Website* juga merupakan media untuk mendapatkan, mencari informasi serta promosi di dunia internet seperti personal, profil sekolah, profil perusahaan, berita pendidikan, bisnis, berita terkini dan semua hal yang dibutuhkan oleh manusia dapat diakses melalui internet. Dengan *website* kita dengan mudahnya menyebarkan dan mendapatkan informasi yang kita butuhkan. *Website* berfungsi sebagai media promosi, media pemasaran, media informasi, media pendidikan,

⁷ Beni Setiawan, *Penegakkan Hukum Pidana Terhadap Akses Sistem Komputer Secara Ilegal (Hacking) Dan Menimbulkan Kejahatan Dunia Maya (Cybercrime) Menurut Prespektif Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik*, tesis Universitas Batanghari, Jambi, 2019.

dan media komunikasi.⁸

Meskipun demikian, dengan melihat banyak sekali manfaat yang diberikan oleh internet seperti manfaat *website* tersebut, hadirnya internet telah memunculkan paradigma baru dalam kehidupan manusia. Kehidupan berubah dari yang hanya bersifat nyata (*real*) ke realitas baru yang bersifat maya (*virtual*). Realitas yang kedua ini biasa dikaitkan dengan internet dan ruang di dunia maya (*cyberspace*).⁹ Internet dengan berbagai kelebihan-kelebihannya juga mempunyai sisi kelemahan dan memiliki dampak buruk jika dipergunakan orang yang tidak bertanggungjawab.

Adanya *cyberspace* yang memberi peluang terjadinya kejahatan atau lebih dikenal dengan *cybercrime* (kejahatan dunia maya), banyak sekali jenis *cybercrime* salah satunya adalah *defacing*. Salah satu tindakan yang mengakibatkan terganggunya sistem elektronik yaitu *Defacing*. *Defacing* merupakan salah satu kejahatan dunia maya yaitu suatu kegiatan yang merubah tampilan suatu *website* orang lain tanpa izin baik halaman utama atau *index filenya* ataupun halaman lain yang masih terkait dalam satu *URL*¹⁰ dengan *website* tersebut (bisa di folder atau di *file*). *Defacing* terdiri dari dua tahap, mula-mula menerobos sistem orang lain atau

⁸ Deni Darmawan dan Deden Hendra Permana, *Desain dan Pemrograman Website*, (Bandung: Remaja Rosdakarya, 2013), 5.

⁹ Abdul Wahid dan Mohammad Labib, *Kejahatan Mayantara (Cybercrime)*, (Jakarta: Refika Aditama, 2005), 103.

¹⁰ *Uniform Resource Locator (URL)*, adalah rangkaian karakter menurut suatu format standar tertentu, yang digunakan untuk menunjukkan alamat suatu sumber seperti dokumen dan gambar di Internet. https://id.wikipedia.org/wiki/Lokator_Sumber_Seragam . diakses pada tanggal 25 Mei 2023 pukul 14.13 WIB

keadaan *web server* dan tahap kedua adalah mengganti halaman *website (web page)* antara *hacking* dan *defacing* tidak dapat terpisahkan satu sama lain, karena *defacing* merupakan salah satu kegiatan *hacking* yaitu, kegiatan menerobos program komputer milik orang atau pihak lain tanpa izin.

Pada awalnya *hacking* tidak selalu berkonotasi negatif, karena sebenarnya tujuan *hacking* adalah untuk mengetahui sistem keamanan milik orang tertentu dan memberi tahu celahnya. Akan tetapi dalam perkembangannya di masyarakat *hacking* dinilai dan dianggap sebuah kata yang mewakili kejahatan dunia maya dan pada kenyataannya memang *hacking* dilakukan tanpa izin.¹¹ Dampak yang ditimbulkan dari adanya tindakan *defacing* ini sangat merugikan bagi pemilik *website* yang diserang oleh *defacer*. Serangan *defacing* yang dilancarkan oleh *attacker* membuat *website* menjadi kacau bahkan tidak berfungsi lagi.

Layanan *website* yang awal mulanya normal menjadi tidak dapat diakses oleh pengguna maupun pemilik *website*. *Password* dan alamat IP untuk login *website* milik *user* tidak bisa digunakan. Kecepatan jaringan pada *website* berkurang karena *defacer* telah melakukan aktivitas *cyber* dalam kapasitas yang besar. Ditemukannya program-program penghancur pada *website user* sehingga akan menurunkan kualitas keamanan *website*. Informasi pada *website* telah bocor karena *defacer* berhasil membobol situs tersebut. Hingga

¹¹ Ahmad Muyassir, *Kejahatan Defacing (Perbandingan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik Dan Hukum Pidana Islam)*, skripsi Universitas Islam Negeri Sunan Kalijaga, Jogja, 2015, 4

yang paling mengkhawatirkan adalah *defacer* memiliki fungsi otoritas di dalam *website*, akibatnya *admin server website* beralih ke tangan *defacer* secara permanen.

Telah banyak terjadi kasus *defacing* di luar negeri dan dalam negeri. Contoh kasus *defacing* yang terjadi di luar negeri yaitu *defacing* yang dilakukan oleh KidsZonk yang berasal dari Indonesia. Puluhan situs diserang oleh *hacker* Indonesia tersebut. Hal ini terjadi akibat dari insiden bendera Indonesia yang terbalik dalam buku panduan SEA Games 2017, imbasnya sebagian besar dari situs milik negara tuan rumah SEA Games 2017 pada waktu itu menampilkan latar belakang berwarna putih dengan gambar bendera Indonesia terbalik seperti yang ada pada buku panduan SEA Games 2017.

Selain itu, gambar lainnya adalah sebuah koran harian yang juga menunjukkan bendera Indonesia yang terbalik. Di bawah gambar ada tulisan: “*Bendera Negeraku Bukanlah Mainan!*” dengan embel-embel telah diretas oleh “KidsZonk”. Tak Cuma itu, *Hacker* juga memasang alunan Indonesia Pusaka sebagai lagu latarnya dan dari puluhan situs yang dikerjai *hacker* tersebut, ada pula yang alamat situsnya dipindahkan ke alamat web lain dengan latar belakang warna hitam.¹²

Indonesia sendiri pun tak luput dari kejahatan *defacing* ini, Pada 27 Juli 2021, perusahaan asuransi BRI *Life* menjadi korban peretasan. Insiden ini membuat sekitar 2 juta data nasabah BRI *Life* diduga bocor dan dijual dengan harga 7.000 dollar AS (sekitar Rp 101,6

¹²<https://www.liputan6.com/amp/3065275/ini-daftar-puluhan-situs-web-malaysia-yang-kena-serangan-hacker>. diakses pada tanggal 27 Mei 2023 pukul 21.36 WIB

juta, kurs 27 Juli 2021) di dunia maya. Kebocoran data ini pertama kali diungkap oleh akun Twitter @UnderTheBreach. Akun tersebut mengklaim bahwa hacker berhasil mengambil 250 GB data dari BRI *Life*, termasuk data 2 juta nasabah dalam format *file* PDF dan sekitar 463.000 dokumen lainnya.

Adapun data nasabah yang bocor berisi informasi seperti foto KTP, rekening, nomor wajib pajak, akte kelahiran, hingga rekam medis. Dugaan kebocoran data ini terjadi karena adanya celah keamanan di dalam sistem elektronik BRI *Life* yang disalahgunakan oleh pihak tak bertanggungjawab. Namun, berdasarkan hasil investigasi internal pihak BRI *Life*, peretasan menargetkan sistem BRI *Life* Syariah. Menurut pihak BRI *Life*, sistem tersebut terpisah dengan sistem inti BRI *Life*.

Dalam kasus lain pada Pada 30 Juli 2021, situs Sekretariat Kabinet (Setkab) Republik Indonesia (RI) yang beralamat setkab.go.id juga menjadi target serangan peretasan dengan metode *deface*. Situs Setkab.go.id tersebut diretas dan tidak bisa diakses.

Kemudian, situs Setkab berubah tampilan menjadi hitam dengan foto yang menampilkan demonstran membawa bendera merah putih dan di bawahnya tertulis keterangan "*Padang Blackhat ll Anon Illusion Team Pwned By Zyy Ft Luthfifake*". Polisi menduga peretasan ini dilakukan demi keuntungan ekonomi. Peretas bertujuan menjual *script backdoor* dari *website* yang jadi target kepada orang yang membutuhkan. Menurut penyelidikan sementara kepolisian, peretasan situs setkab.go.id terjadi akibat kelemahan pada sistem keamanan dan kelengahan operator. Lalu, seminggu

setelah peretasan, situs Setkab sudah kembali ke tangan pemerintah. Pihak Setkab memastikan tidak ada dokumen rahasia pada situs Setkab.¹³

Kasus *Defacing* lainnya yang menimpa Pengadilan Negeri Unahaa, yaitu pada hari Sabtu, tanggal 30 Juni 2018, sebuah peristiwa yang mengganggu ketenangan Pengadilan Negeri Unahaa terjadi di provinsi Sulawesi Tenggara. Pukul 20.00 WIB. Yoga dengan sengaja merusak sistem elektronik pengadilan tersebut. Dia melakukan *defacing* pada situs web pengadilan setelah mencari celah keamanan dengan menggunakan laptop Acer miliknya dan mencari bug melalui mesin pencari Google. Yoga menemukan celah di situs jdih1.pn-unaaha.go.id dan mengubah tampilan halaman secara ilegal. Tindakan ini mengganggu operasional pengadilan dan merugikan integritas sistem elektroniknya.

Aksi *defacing* yang dilakukan oleh Yoga ini tentu saja adalah suatu pelanggaran serius terhadap hukum. Pengadilan Negeri Unahaa mengalami gangguan pada sistem elektroniknya, yang dapat mengganggu tugas-tugas penting dan kredibilitas pengadilan dalam menjalankan fungsinya. Yoga, dengan menggunakan pengetahuannya untuk merusak dan mengambil keuntungan dari celah dalam keamanan, telah melakukan tindakan ilegal yang dapat berdampak merugikan banyak pihak. Serangkaian kejahatan *defacing* yang telah disebutkan di atas bukanlah masalah yang sepele, perlu adanya aturan aturan yang memberikan batasan dan

¹³<https://tekno.kompas.com/read/2021/12/21/06540017/8-kasus-peretasan-yang-terjadi-di-indonesia-sepanjang-2021?page=all#page2>. diakses pada tanggal 25 Mei 2023 pukul 22.20 WIB

ancaman terhadap tindakan tersebut.

Adanya Undang-undang ITE yang menjadi instrumen sangat diperlukan dalam upaya mencegah dan menindak tindakan seperti *defacing*. Indonesia yang mayoritas penduduknya beragama Islam dan Islam sendiri menjunjung tinggi adab, tata krama serta hukum tentunya mempunyai andil untuk mengikuti fenomena yang terjadi di masyarakat, termasuk akibat buruk yang ditimbulkan dari perkembangan informasi, serta mengharuskan hukum Islam yang menjawab permasalahan tersebut dan mengingat hukum Islam yang berkembang seiring berjalannya waktu dan tempat. Islam sendiri juga menghormati hak pribadi atau *privacy* seseorang seperti dalam ayat Al-Qur'an berikut ini :

﴿يَا أَيُّهَا الَّذِينَ آمَنُوا لَا تَدْخُلُوا بُيُوتًا غَيْرَ بُيُوتِكُمْ حَتَّى تَسْتَأْذِنُوا
وَتُسَلِّمُوا عَلَىٰ أَهْلِهَا ذَلِكُمْ خَيْرٌ لَّكُمْ لَعَلَّكُمْ تَذَكَّرُونَ ٢٧ فَإِنْ لَمْ
تَجِدُوا فِيهَا أَحَدًا فَلَا تَدْخُلُوهَا حَتَّىٰ يُؤْذَنَ لَكُمْ وَإِنْ قِيلَ لَكُمْ ارْجِعُوا
فَارْجِعُوا هُوَ أَزْكَىٰ لَكُمْ يٰۤأَيُّهَا الَّذِينَ آمَنُوا عَمَلُوكُمُ اللَّيْلُ نِهَاكُمْ

“Wahai orang-orang yang beriman, janganlah memasuki rumah yang bukan rumahmu sebelum meminta izin dan memberi salam kepada penghuninya. Demikian itu lebih baik bagimu agar kamu mengambil pelajaran.” (Q.S An-Nur : 27)

“Jika kamu tidak menemui seorang pun di dalamnya, janganlah masuk sebelum mendapat izin. Jika dikatakan kepadamu, “Kembalilah,” (hendaklah) kamu kembali. Itu lebih suci bagimu. Allah Maha Mengetahui apa yang kamu kerjakan.” (Q.S An-Nur : 28)

Ayat di atas menjelaskan tentang larangan masuk

rumah tanpa izin, Ayat di atas menjelaskan larangan memasuki rumah tanpa izin, dari hal ini dapat dilihat bahwa pelanggaran terhadap privasi dilarang, sehingga melakukan *defacing* juga tidak boleh dilakukan. Tahap pertama dari *defacing* melibatkan *hacking* untuk membobol *website* orang lain, dan tahap kedua adalah mengganti halaman *website* (*web page*). Islam selalu mendorong etika dan tata krama yang baik terhadap orang lain. Oleh karena itu, tindakan seperti Perundangan dunia maya (*Defacing*) dianggap sebagai perbuatan yang diharamkan, terutama karena dampaknya dapat menyebabkan kerugian bagi orang lain. Hal ini menjadi lebih serius jika target *defacing* adalah *website* milik pemerintah, yang bisa berpotensi menimbulkan kerugian besar dan merupakan tindakan yang sangat dzalim.¹⁴

Islam sendiri melarang keras sesama muslim saling mendalimi satu sama lain, banyak ayat ayat yang menegaskan orang yang dzalim akan di timpahkan dosa yang sangat besar dan sangat keras siksaannya diakhirat kelak nanti. Salah satu surah dalam Qur'an yang menunjukkan balasan orang orang dzalim dalam (Surah Yunus (10):52) Allah SWT berfirman :

﴿ ثُمَّ قِيلَ لِلَّذِينَ ظَلَمُوا ذُوقُوا عَذَابَ الْخُلْدِ هَلْ تُجْرُونَ إِلَّا بِمَا كُنْتُمْ

تَكْسِبُونَ ﴿٥٢﴾

“Kemudian, dikatakan kepada orang-orang yang zalim

¹⁴ M.Ade Chairuddin Najib, *Sanksi Terhadap Tindak Pidana Defacing Dalam Undang Undang Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik Dengan Prespektif Hukum Islam*, skripsi Universitas Islam Negeri Raden Fatah, Palembang, 2018, 84-86.

itu, “Rasakanlah olehmu azab yang kekal. (Bukankah kamu tidak diberi balasan, melainkan (setimpal) dengan apa yang selama ini telah kamu usahakan?”

Dengan demikian, menjadi sangat jelas bagi kita betapa signifikannya peran Islam dalam mendidik umat Muslim agar memiliki akhlak yang mulia dan menjauhi perilaku-perilaku yang tercela seperti yang telah disebutkan. Islam mendorong agar umat Muslim memiliki akhlak yang baik dan menjauhi perbuatan yang tercela tersebut. Lebih dari itu, Islam mengharapkan agar umat Muslim hidup dalam suasana persaudaraan yang dipenuhi dengan kasih sayang dan kepercayaan satu sama lain.¹⁵ Penanggulangan gangguan keamanan dan penyelenggaraan sistem secara elektronik dalam menggunakan pendekatan hukum yang bersifat mutlak karena tanpa kepastian hukum, persoalan pemanfaatan teknologi informasi menjadi tidak optimal.

Maka dari itu, pemerintah mengesahkan Undang-undang pada tanggal 28 April 2008 dan melakukan perubahannya pada tanggal 25 November 2016 sehingga lahirlah Undang-Undang Nomor 11 tahun 2008 sebagaimana telah diubah menjadi Undang-Undang Nomor 19 tahun 2016 Tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik untuk memenuhi kebutuhan hukum tersebut dan agar semua kejahatan mayantara dapat terakomodir oleh Undang-undang tersebut.

Dalam hal ini, UU ITE telah menetapkan perbuatan-

¹⁵ M.Ade Chairuddin Najib, *Sanksi Terhadap Tindak Pidana Defacing Dalam Undang Undang Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik Dengan Prespektif Hukum Islam*, skripsi Universitas Islam Negeri Raden Fatah, Palembang, 2018, hal 87-88.

perbuatan mana yang termasuk tindak pidana di bidang ITE dan telah ditentukan sifat jahatnya dan penyerangan terhadap berbagai kepentingan hukum dalam bentuk rumusan-rumusan tindak pidana tertentu.¹⁶

Melihat urgensi permasalahan tersebut, penulis tertarik untuk melakukan penelitian dan analisis yuridis terhadap putusan pengadilan Nomor 25/Pid.Sus/2019/Pn Unh terkait tindak pidana yang berakibat terganggunya sistem elektronik. Penelitian ini diharapkan dapat memberikan kontribusi dalam rangka penegakan hukum, kepastian hukum, dan keadilan bagi masyarakat dalam menghadapi ancaman *cybercrime*, khususnya tindak pidana yang mengganggu sistem elektronik. Secara keseluruhan dari pemaparan latar belakang di atas bahwa penelitian tentang perbuatan tindak pidana yang mengakibatkan rusaknya sistem elektronik ini sangatlah penting, terutama dalam dunia yang terus berkembang dengan teknologi canggih serta hukum yang bertambah rumit. Penulis tertarik meneliti secara mendalam terkait kasus tindak pidana yang berakibat terganggunya sistem elektronik. Maka skripsi ini memiliki judul “*Analisis Yuridis Terhadap Tindak Pidana Yang Berakibat Terganggunya Sistem Elektronik (Studi Putusan Nomor 25/Pid.Sus/2019/PN Unh)*”.

B. Rumusan Masalah

Berdasarkan latar belakang masalah di atas, fokus penelitian penulis adalah untuk menganalisis secara yuridis tindak pidana yang mengakibatkan terganggunya

¹⁶ Adami Chazawi dan Ferdian Adi, *Tindak Pidana Informasi dan Transaksi Elektronik*, (Malang, Media Nusa Creative, 2015), 3

sistem elektronik, khususnya dalam konteks putusan Nomor 25/Pid.Sus/2019/PN Unh. Maka dari itu, rumusan masalah penulis adalah:

1. Bagaimana pertimbangan hukum hakim terhadap tindak pidana yang berakibat terganggunya sistem elektronik dalam putusan Pengadilan Negeri Unaha Nomor 25/Pid.Sus/2019/PN Unh?
2. Bagaimana analisis terhadap tindak pidana yang berakibat terganggunya sistem elektronik dalam Putusan Pengadilan Negeri Unaha Nomor 25/Pid.Sus/2019/PN Unh?

C. Tujuan Penelitian

Berdasarkan rumusan masalah tersebut maka tujuan penelitian yang berusaha dicapai oleh penulis adalah sebagai berikut:

1. Untuk mengetahui pertimbangan hukum hakim terhadap tindak pidana yang berakibat terganggunya sistem elektronik dalam putusan Pengadilan Negeri Unaha Nomor 25/Pid.Sus/2019/PN Unh.
2. Untuk mengetahui analisis terhadap tindak pidana yang berakibat terganggunya sistem elektronik dalam Putusan Pengadilan Negeri Unaha Nomor 25/Pid.Sus/2019/PN Unh.

D. Manfaat Penelitian

Dalam penelitian ini terdapat 2 (dua) manfaat penelitian yang berusaha untuk penulis wujudkan, manfaat tersebut terdiri dari manfaat teoritis dan manfaat praktis yang diuraikan sebagai berikut ini:

1. Manfaat Teoretis

- a. Penelitian ini dapat memberikan kontribusi pada pengembangan ilmu hukum, khususnya dalam bidang hukum pidana dan teknologi informasi.
- b. Hasil analisis dapat memperkaya pemahaman tentang pertimbangan hukum hakim dalam kasus-kasus yang melibatkan gangguan sistem elektronik.
- c. Diharapkan studi ini dapat menjadi referensi bagi penelitian-penelitian selanjutnya terkait *cybercrime* dan penerapan UU ITE.

2. Manfaat Praktis

Dari aspek praktis, hasil ini diharapkan dapat menjadi sumbangsih untuk referensi bagi penelitian selanjutnya, sehingga penulis berharap bahwa penelitian ini dapat memberikan wawasan ilmu pengetahuan mengenai tindak pidana yang mengakibatkan terganggunya sistem elektronik serta agar memiliki pemahaman yang lebih baik tentang tindak pidana terkait teknologi atau *cybercrime*, dapat membantu dalam meningkatkan kesadaran hukum di masyarakat terkait dengan tindakan yang dapat merusak sistem elektronik. Hal ini dapat berkontribusi pada pencegahan tindakan pidana semacam itu. Lebih lanjut, penelitian ini bertujuan untuk meningkatkan pemahaman yang lebih komprehensif tentang tindak pidana terkait teknologi atau *cybercrime*. Dengan menyajikan analisis mendalam tentang kasus konkret, studi ini dapat membantu praktisi hukum, penegak hukum, dan

pemangku kepentingan lainnya dalam memahami kompleksitas dan nuansa hukum dari kejahatan siber.

E. Telaah Pustaka

Telaah Pustaka digunakan untuk mendapatkan gambaran tentang hubungan pembahasan dengan penelitian yang pernah dilakukan oleh peneliti sebelumnya, serta untuk memperoleh gambaran terkait korelasi dari pembahasan dengan penelitian yang sudah pernah dilaksanakan dari peneliti sebelumnya. Sehingga tidak terjadi pengulangan dan plagiasi karya ilmiah yang pernah ada. Telaah Pustaka yang dimaksud yakni mengenai permasalahan terhadap tindak pidana yang mengakibatkan terganggunya sistem elektronik.

Pertama, skripsi M Ade Chairuddin Najib pada tahun 2018 yang berjudul “Sanksi Terhadap Tindak Pidana *Defacing* Dalam Undang Undang Nomor 19 Tahun 2016 tentang Informasi dan transaksi elektronik Dengan Prespektif Hukum Islam”.¹⁷ dalam skripsi ini membahas *Defacing* merupakan kejahatan siber dengan mengubah tampilan *website* orang lain tanpa izin melalui penerobosan sistem. Maraknya kejahatan ini menjadi fenomena baru yang menarik untuk dikaji dari perspektif hukum pidana Indonesia dan fiqih jinayah. Penelitian ini merupakan penelitian kepustakaan dengan menganalisis data secara deskriptif analitik komparatif. Pendekatan yang digunakan adalah yuridis normatif, yaitu mendekati

¹⁷ M.Ade Chairuddin Najib, *Sanksi Terhadap Tindak Pidana Defacing Dalam Undang Undang Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik Dengan Prespektif Hukum Islam*, skripsi Universitas Islam Negeri Raden Fatah, Palembang, 2018.

masalah *defacing* dari segi hukum yang terdapat dalam Undang-Undang dan hukum Islam. Berdasarkan metode yang digunakan, ditemukan bahwa menurut Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE), *defacing* merupakan perbuatan yang dilarang sebagaimana diatur dalam Pasal 30 dan Pasal 32 ayat (1). Dalam hukum Islam, *defacing* juga dilarang karena merugikan dan memberi madarat bagi orang lain. Meskipun tidak ada dalil secara langsung, *defacing* dikategorikan sebagai jarimah ta'zir dalam hukum Islam. Sanksi tindak pidana *defacing* menurut UU ITE diatur dalam Pasal 46 dan Pasal 48 ayat (1). Dalam hukum Islam, *defacing* masuk kategori jarimah ta'zir, sehingga jenis dan besaran hukumannya diserahkan kepada ulil amri atau hakim sesuai dengan kemaslahatan. Perbedaan dengan skripsi yang ditulis yaitu penulis berfokus mengkaji *defacing* dalam suatu kasus yang dilakukan terdakwa yaitu mengubah tampilan *website* milik Pengadilan Negeri Unaha, pertimbangan hakim, serta tepat atau tidaknya hakim dalam penerapan hukum pidana dalam suatu putusan dengan nomor perkara 25/Pid.Sus/2019/PN.Unh dan tidak menggunakan perspektif dari hukum pidana Islam.

Kedua, skripsi yang ditulis oleh Ahmad Muyasir pada tahun 2015 dengan judul “Kejahatan *Defacing* (Perbandingan Undang-Undang nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik dan Hukum Pidana Islam)” membahas tentang kejahatan *cyber* yaitu *defacing*, yang merupakan tindakan merubah tampilan *website* orang lain tanpa izin dengan cara menerobos sistem terlebih dahulu. Penelitian ini bertujuan untuk

mengetahui pandangan hukum pidana Indonesia (UU ITE) dan hukum Islam (fikih jinayah) terhadap tindak pidana *defacing*, serta membandingkan keduanya. Penelitian ini merupakan penelitian kepustakaan dengan analisis deskriptif komparatif menggunakan pendekatan yuridis normatif. Hasilnya, menurut UU ITE No.11 Tahun 2008, *defacing* dilarang dalam Pasal 30 (menerobos sistem tanpa izin) dan Pasal 32 ayat 1 (memodifikasi *website* tanpa hak). Dalam Islam, *defacing* juga dilarang karena merugikan orang lain dan masuk kategori jarîmah ta'zîr karena tidak ada dalil khusus. Sanksi *defacing* menurut UU ITE diatur dalam Pasal 46 dan 48 ayat 1, sedangkan dalam Islam, hukumannya ditentukan oleh hakim/ulil amri sesuai dengan kemaslahatan.¹⁸

Ketiga, skripsi yang ditulis oleh Hartoto Suci Rahayu pada tahun 2021 berjudul “Tinjauan Yuridis Tindak Pidana *Defacing* dalam Perspektif Hukum Pidana di Indonesia (Studi Kasus Putusan Pengadilan Negeri Surakarta Nomor 399/Pid.Sus/2017/PN Skt.)”¹⁹, dalam skripsi ini membahas membahas tentang tindak pidana *defacing*, yaitu kejahatan *cyber* dengan cara mengubah tampilan sistem elektronik/komputer melalui penerobosan secara ilegal. Tujuan penelitian ini adalah untuk mengkaji batasan norma dalam tindak pidana

¹⁸ Ahmad Muyassir, *Kejahatan Defacing (Perbandingan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik Dan Hukum Pidana Islam)*, skripsi Universitas Islam Negeri Sunan Kalijaga, Jogja, 2015.

¹⁹ Hartoto Suci Rahayu, *Tinjauan Yuridis Tindak Pidana Defacing Dalam Prespektif Hukum Pidana Di Indonesia (Studi Putusan Pengadilan Negeri Surakarta Nomor 399/Pid.Sus/2017/Pn.Skt)*, skripsi Universitas Sebelas Maret, Surakarta, 2021.

defacing berdasarkan hukum pidana Indonesia dan menganalisis pertimbangan hakim dalam Putusan Pengadilan Negeri Surakarta No. 399/Pid.Sus/2017/PN Skt terkait kasus *defacing website* Dewan pers. Penelitian ini merupakan penelitian yuridis normatif yang bersifat preskriptif dan terapan, dengan menggunakan pendekatan peraturan perundang-undangan dan pendekatan kasus. Data yang digunakan meliputi bahan hukum primer, sekunder dan tersier yang dikumpulkan melalui studi kepustakaan, serta dianalisis dengan metode silogisme dan interpretasi. Hasilnya, tindak pidana *defacing* dibatasi oleh 14 perbuatan seperti mengakses, melanggar, menerobos, mengubah, merusak, memindahkan dsb sistem elektronik/komputer secara sengaja dan melawan hukum. Pertimbangan hakim dalam putusan tersebut dinilai mengabaikan fakta bahwa terdakwa tidak mendapat keuntungan, sehingga hukuman 2 tahun dinilai kurang adil.

Keempat, karya tulis yang berbentuk jurnal yang ditulis oleh Muhammad Anthony Aldriano, Mas Agus Priyambodo, dalam jurnal Kewarganegaraan pada tahun 2022 yang berjudul “*Cyber Crime Dalam Sudut Pandang Hukum Pidana*”²⁰, dalam karya tulis ini membahas membahas tentang pentingnya kebijakan hukum untuk menanggulangi *cybercrime*. Perkembangan teknologi yang pesat telah membuka peluang baru bagi para penjahat untuk melakukan kejahatan di dunia maya. Hal ini menjadi tantangan bagi penegak hukum karena

²⁰ Muhammad Anthony Aldriano dan Mas Agus Priyambodo, “*Cyber Crime Dalam Sudut Pandang Hukum Pidana*”, Vol. 6 No. 1, *Jurnal Kewarganegaraan*, 2022.

cybercrime memiliki karakteristik yang berbeda dengan kejahatan tradisional serta menekankan pentingnya kebijakan hukum yang tepat untuk mengatasi *cybercrime*. Kebijakan hukum tersebut harus mempertimbangkan fakta hukum terbaru dan dampak dari penyalahgunaan ilmu pengetahuan dan teknologi. Kebijakan hukum ini juga harus mengatur mengenai sistem pembuktian dalam kasus *cybercrime*.

F. Metode Penelitian

Menurut Sugiyono dalam bukunya yang berjudul “Teori Metode Dasar” menyatakan bahwa penelitian adalah salah satu cara yang paling jitu dalam usaha untuk mengembangkan standar dan tatanan yang ada, dalam suatu penelitian membutuhkan suatu metode yang diuraikan sebagai berikut:²¹

1. Jenis Penelitian dan Pendekatan Penelitian

Penelitian yang dilakukan penulis menggunakan jenis penelitian *juridic normatif*. Penelitian *Juridic normatif* sendiri terbagi menjadi 3, penelitian terhadap asas hukum (*doktrinal*), penelitian terhadap sistematika hukum, dan penelitian pada taraf sinkronisasi hukum.²² Penulis dalam hal ini menggunakan jenis penelitian *Doktrinal*.

Penelitian *Doktrinal* yaitu penelitian-penelitian atas hukum yang didasarkan pada doktrin-doktrin yang dikonsepsikan oleh pengonsepanya dan berkembang dalam ilmu hukum. Penelitian doktrinal

²¹ Sugiyono, *Teori Metode Dasar*, (Jakarta: Gramedia, 2019), 31.

²² Zainudin Ali, *Metode Penelitian Hukum*, (Jakarta: Sinar Grafika, 2014), 24.

di Indonesia sudah lazim disebut dengan penelitian normatif yang mengkaji dan menelaah pokok permasalahan dengan norma hukum dan kaidah hukum yang berlaku di dalam hukum positif.

Sementara itu, dalam penelitian ini menggunakan pendekatan perundang-undangan (*statute approach*) dan pendekatan konseptual (*conceptual approach*). Pendekatan perundang-undangan (*statute approach*) yaitu menelaah semua peraturan perundang-undangan yang berkaitan dengan masalah yang dibahas sehingga dari hasil telaah akan memberikan jawaban dari isu yang menjadi pokok bahasan.²³ Pendekatan konseptual (*conceptual approach*) merupakan pendekatan penelitian dengan menelaah pokok masalah dengan mengkaji doktrin-doktrin ilmu hukum, asas hukum, dan konsep hukum yang relevan dengan isu yang dihadapi.²⁴

2. Sumber Data dan Bahan Hukum

Sumber data dalam penulisan penelitian ini menggunakan jenis data sekunder. Data sekunder yaitu sebuah proses yang dilakukan dengan menganalisis sebuah data tanpa harus melakukan wawancara, survei, hingga observasi dalam memperoleh sebuah data. Data sekunder adalah sebuah data yang didapat dari buku yang telah dipublikasikan oleh orang lain, atau juga dapat diperoleh dari dokumen dan hasil penelitian yang telah dilakukan peneliti sebelumnya. Data sekunder yaitu sebuah data atau keterangan yang kita peroleh secara tidak langsung dengan cara

²³ Peter Mahmud Marzuki, *Penelitian Hukum*, (Jakarta: Kencana, 2005), 93.

²⁴ Peter Mahmud Marzuki, *Penelitian Hukum*, (Jakarta: Kencana, 2005), 95.

mengutip dari Undang- Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektornik serta Undang-Undang Nomor 16 Tahun 2016 Tentang Perubahan Informasi dan Transaksi Elektronik.

Dalam melakukan penelitian tersebut penulis menggunakan 3 (tiga) bahan hukum yaitu bahan hukum primer, bahan hukum sekunder, dan bahan hukum tersier, ketiga bahan hukum tersebut dikumpulkan melalui studi kepustakaan dengan penjelasan sebagai berikut:

Bahan Hukum Primer

Bahan hukum primer merupakan bahan hukum yang mengikat atau yang membuat orang taat pada hukum seperti peraturan perundang-undangan, dan putusan hakim. Bahan hukum primer yang penulis gunakan di dalam penulisan ini yakni Undang-undang Dasar Negara Republik Indonesia Tahun 1945, Undang-undang Nomor 1 Tahun 1946 Tentang Peraturan Hukum Pidana (selanjutnya disebut KUHP) dan Undang-undang Nomor 19 Tahun 2016 Tentang Perubahan Informasi dan Transaksi Elektronik, Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, Putusan Pengadilan Negeri Unahaa Nomor 25/Pid.Sus/2019/PN. Unh.

a. Bahan Hukum Sekunder

Bahan hukum sekunder itu diartikan sebagai bahan hukum yang tidak mengikat tetapi menjelaskan mengenai bahan hukum primer yang merupakan hasil olahan pendapat atau pikiran para pakar atau ahli yang mempelajari suatu bidang tertentu secara khusus yang akan memberikan petunjuk ke mana peneliti akan mengarah. Yang

dimaksud dengan bahan sekunder disini oleh penulis adalah buku buku ilmiah dari penulis ahli hukum, jurnal-jurnal hukum, hasil penelitian hukum, artikel hukum, dan literasi dari media massa maupun media internet dan sumber hukum lain yang mendukung penulisan hukum ini.

b. Bahan Hukum Tersier

Bahan Hukum Tersier Bahan hukum tersier yaitu bahan hukum yang merupakan pelengkap yang sifatnya memberikan petunjuk atau penjelasan tambahan terhadap bahan hukum primer dan sekunder. Bahan hukum tersier yang terdapat dalam penelitian misalnya kamus hukum, kamus besar bahasa Indonesia.

3. Teknik Pengumpulan Data

Teknik pengumpulan data adalah teknik penelitian untuk mengumpulkan berbagai data dan informasi. Teknik pengumpulan data dalam penelitian ini menggunakan studi kepustakaan (*Library Research*). Studi kepustakaan (*Library Research*) yaitu sebuah teknik pengumpulan data dengan cara menganalisis dokumen untuk mengumpulkan data yang bersumber dari kepustakaan. Teknik pengumpulan data yang dilakukan dalam penelitian ini dilakukan dengan cara mengkaji data melalui sumber yang berasal dari UU ITE No.19 Tahun 2016, KUHP, literatur, jurnal ilmiah, teori-teori, dan *website* yang berkaitan dengan penelitian ini.²⁵

4. Analisis Data

Teknik analisis data adalah metode dalam memproses data menjadi informasi. Teknik analisis data yang

²⁵ Soerjono Soekanto, dkk, *Penelitian Hukum Normative Suatu Tinjauan Singkat*, (Jakarta: Raja Grafindo Persada, 2008), 13-14.

digunakan dalam penelitian yuridis normatif berlandaskan kepada teknik analisis kualitatif. Teknik analisis kualitatif adalah teknik analisis yang digunakan dengan cara menguraikan data secara bermutu dalam bentuk kalimat yang teratur, logis, efektif dan tidak tumpang tindih sehingga memudahkan dalam memahami sebuah data.

G. Sistematika Penulisan

Untuk mempermudah penulisan skripsi yang diperlukan suatu sistematika penulisan agar pembahasannya lebih tersusun dan terarah yaitu:

Bab pertama Pendahuluan. Pada bab I ini, berisi tentang penelitian yang meliputi latar belakang, rumusan masalah, tujuan penulisan, manfaat penulisan, telaah pustaka, metode penelitian, dan sistematika penulisan

Bab kedua. Pada bab II ini, membahas tentang Tinjauan konseptual Tindak Pidana. Perbuatan yang berkibat terganggunya sistem elektronik (*defacing*). Pengertian *defacing*, dampak *defacing*, penyebab terjadinya *defacing*, metode *defacing*, cara kerja dan jenis jenis *defacing*. Pengertian Hukum Pidana.

Bab ketiga Data Penelitian. Pada bab III ini, merupakan penyajian data mengenai tentang duduk perkara pada putusan Pengadilan Negeri Nomor 25/Pid.Sus/2019/PN.Unh tentang tindak pidana yang berakibat terganggunya sistem elektronik.

Bab keempat Analisis Putusan. Pada bab IV ini menjelaskan tentang pertimbangan hukum hakim terhadap tindak pidana yang berakibat terganggunya sistem elektronik dan analisis yuridis terhadap tindak pidana yang berakibat terganggunya sistem elektronik

dalam Putusan Nomor 25/Pid.Sus/2019/PN Unh.

Bab kelima Penutup. Pada bab V ini, Merupakan penutup yang berisi simpulan dari penelitian yang menjadi jawaban dari rumusan masalah serta saran-saran.

BAB II

TINJAUAN TEORITIK TENTANG TINDAK PIDANA, KEJAHATAN DUNIA MAYA (*CYBER CRIME*), SISTEM ELEKTRONIK

A. Tindak Pidana

1. Pengertian

Istilah “*strafbaar feit*” dalam hukum pidana memiliki berbagai macam dalam penggunaan bahasa Indonesia. Moeljatno mengartikan “*strafbaar feit*” sebagai “perbuatan pidana”, sementara dalam pandangan para ahli hukum pidana di Indonesia, istilah ini disamakan pengertiannya sebagai “tindak pidana”.¹ Tindak pidana sendiri pada hakikatnya merupakan istilah yang berasal dari Belanda, terjemahan dari kata *Strafbaar feit*, kadang-kadang juga *delict* yang berasal dari bahasa Latin *delictum*.² Tindak pidana merupakan pengertian dasar dalam hukum pidana (yuridis normatif). Kejahatan atau perbuatan jahat bisa diartikan secara yuridis atau kriminologis. Kejahatan atau perbuatan jahat dalam arti yuridis normatif adalah perbuatan seperti yang terwujud *in abstracto* dalam peraturan pidana.³

Istilah *feit* pada bahasa Belanda artinya yakni “sebagian dari suatu kenyataan” atau “*een gedeelte van de werkelijkheid*”, sementara “*strafbaar*” berarti “dapat

¹ Agus Rusianto, *Tindak Pidana & Pertanggungjawaban Pidana Tinjauan Kritis Melalui Konsistensi Antara Asas, Teori, Dan Penerapannya*, 1st ed. (Jakarta: Prenadamedia, 2016), 11. (Rusianto, 2016) (Ishaq, 2020) (Mertokusumo, 1999) (Hamzah, 2001) (Muhammad, 2009) (Suyanto, 2018) (Effendi. & Jonaedi, 2016)

² Ishaq, *Hukum Pidana*, (Depok: Rajawali Pers, 2020), 71.

³ Sudikno Mertokusumo, *Mengenal Hukum*, (Liberty, Yogyakarta, 1999), 10.

dihukum”, hingga menurut harfiah istilah *strafbaar feit* bisa diartikan menjadi “sebagian dari suatu kenyataan yang dapat dihukum” yang pasti sudah sesuai sebab jika diketahui yakni yang bisa mendapat hukuman ialah manusia sebagai pribadi serta bukanlah perilaku, kenyataan, maupun tindakan.

Dari Undang-Undang yang sudah ada saat ini sudah umum diketahui, *strafbaar feit* diartikan sama dengan “tindak pidana” dalam bahasa Indonesia. Terminologi *strafbaar feit* diartikan sama dengan “tindak pidana” yang bertujuan untuk memudahkan memaknainya sebab istilah tindak pidana telah diketahui di beberapa aturan perundang-undangan ataupun telah dikemukakan beberapa ahli hukum pidana pada literatur-literturnya. Pemakaian terminologi “tindak pidana” memiliki tujuan untuk membuat konsistensi penulisan terkait terminologi *strafbaar feit*, agar lebih mudah ketika memakai istilah “tindak pidana” bukannya “perbuatan pidana” maupun “peristiwa pidana”⁴

Tindak pidana adalah suatu kelakuan manusia yang dirumuskan dalam Undang-Undang, melawan hukum, serta memiliki akibat hukum yang patut dipidana dan dilakukan dengan unsur kesalahan. Bagi siapa saja yang melakukan perbuatan pidana harus mempertanggungjawabkan perbuatannya.⁵

Tindak pidana merupakan perbuatan yang dilarang oleh hukum dan diancam dengan sanksi pidana. Istilah tindak pidana berasal dari bahasa Belanda, *strafbaar feit*,

⁴ Agus Rusianto, *Tindak Pidana &....* 12.

⁵ Andi Hamzah, *Bunga Rampai Hukum Pidana dan Acara Pidana*, (Jakarta, Ghalia Indoensia, 2001), 22.

yang berarti perbuatan yang dapat dihukum. Istilah lain yang digunakan adalah *delict*, yang berasal dari bahasa Latin, *delictum*, yang berarti kesalahan.⁶ Muljanto, mengatakan perbuatan pidana adalah tindakan yang melanggar peraturan perundang-undangan dan dikenai hukuman. Tindakan ini dapat berupa suatu kejadian yang ditimbulkan oleh orang. Hukuman ditujukan kepada orang yang menimbulkan kejadian tersebut.

Hubungan antara larangan dan hukuman sangat erat, karena hubungan antara kejadian dan orang yang menimbulkan kejadian juga sangat erat. Kejadian tidak dapat dilarang jika tidak ada orang yang menimbulkannya, dan orang tidak dapat dihukum jika tidak melakukan kejadian tersebut. Untuk menyatakan hubungan yang erat antara larangan, kejadian, dan hukuman, maka digunakan istilah “perbuatan pidana”. Istilah ini merupakan pengertian abstrak yang mencakup dua keadaan konkret: pertama, adanya kejadian tertentu, dan kedua, adanya orang yang berbuat dan menimbulkan kejadian tersebut.

Menurut Simons, menerangkan bahwa *strafbaar feit* adalah kelakuan (*handeling*) yang diancam dengan pidana, yang bersifat melawan hukum, yang berhubungan dengan kesalahan dan yang dilakukan oleh orang yang mampu bertanggung jawab. Menurut Van Hamel, merumuskan *strafbaar feit* sebagai kelakuan orang (*menselijke gedraging*) yang dirumuskan dalam *wet*, yang bersifat melawan hukum, yang patut dipidana (*strafwaarding*) dan

⁶ Nurul Irfan Muhammad. “Tindak Pidana Korupsi di Indonesia Dalam Perspektif Fiqh Jinayah”, (Jakarta: Badan Litbang dan Diklat Departemen Agama RI, 2009), 31.

dilakukan dengan kesalahan. Jika melihat pengertian-pengertian ini, maka di situ dalam pokoknya ternyata:

- a. Bahwa *feit* dalam *strafbaar feit* berarti *handeling*, kelakuan atau tingkah laku
- b. Bahwa pengertian *strafbaar feit* dihubungkan dengan kesalahan orang yang mengadakan kelakuan tadi.⁷

Sementara dalam berbagai perundang-undangan sendiri digunakan berbagai istilah untuk menunjukkan pada pengertian kata *strafbaarfeit*. Beberapa istilah yang digunakan dalam undang-undang tersebut antara lain:

- a. Peristiwa Pidana, istilah ini antara lain digunakan dalam Undang-Undang Dasar Sementara (UUDS) tahun 1950 khususnya dalam pasal 14.
- b. Perbuatan Pidana, istilah ini digunakan dalam Undang-undang Nomor 1 Tahun 1952 tentang Tindakan Sementara untuk menyelenggarakan kesatuan susunan, kekuasaan, dan acara pengadilan-pengadilan sipil.
- c. Perbuatan-perbuatan yang dapat dihukum, istilah ini digunakan dalam Undang-undang Darurat Nomor 2 Tahun 1951 tentang Perubahan Ordonantie Tijdelike Byzondere Strafbepalingen.
- d. Hal yang diancam dengan hukum, istilah ini digunakan dalam Undang-undang Darurat Nomor 16 Tahun 1951 tentang Penyelesaian Perselisihan Perburuhan.
- e. Tindak Pidana, istilah ini digunakan dalam berbagai undang-undang, misalnya:

⁷ Suyanto, *Pengantar Hukum Pidana*, (Yogyakarta, CV BUDI UTAMA, 2018), 68-69.

- 1) Undang-undang Darurat Nomor 7 Tahun 1953 tentang Pemilihan Umum
- 2) Undang-undang Darurat Nomor 7 Tahun 1953 tentang Pengusutan, Penuntutan, dan Peradilan Tindak Pidana Ekonomi
- 3) Penetapan Presiden Nomor 4 Tahun 1953 tentang kewajiban Kerja Bakti dalam rangka pemasyarakatan bagi terpidana karena melakukan tindak pidana yang merupakan kejahatan.⁸

2. Unsur-Unsur

Tindak pidana adalah perbuatan yang melanggar undang-undang dan dikenai sanksi pidana. Sanksi pidana tersebut merupakan ancaman yang diberikan oleh undang-undang kepada orang yang melakukan perbuatan tersebut. Untuk menentukan apakah suatu perbuatan merupakan tindak pidana, maka perbuatan tersebut harus diatur dalam undang-undang. Undang-undang tersebut harus memuat unsur-unsur yang menjadi ciri atau sifat perbuatan tersebut, sehingga dapat dibedakan dari perbuatan lain yang tidak dilarang.

Teori hukum pidana mengenal dua pendirian tentang pengertian dan unsur-unsur tindak pidana. Pendirian yang pertama dikenal sebagai pendirian atau aliran monistis, sedangkan pendirian atau aliran kedua adalah pendirian atau aliran dualistis. Pembahasan tentang kedua aliran ini diperlukan dalam memahami pemahaman secara akademis atau teoretis tentang

⁸ Effendi, Jonaedi. *Cepat & Mudah Memahami Hukum Pidana*. (Jakarta, Prenada Media, 2016), 36-37.

pengertian dan unsur-unsur tindak pidana terutama dalam kaitannya dengan syarat syarat pemidanaan.

Berdasarkan wawasan hukum pidana, sesuatu perilaku bisa termasuk *een doen* atau *een niet doen* atau bisa termasuk “hal melakukan sesuatu” maupun “hal tidak melakukan sesuatu”, yang terakhir didalam doktrin pun juga dikenal dengan *een nalaten* yang memiliki arti “hal mengalpakan sesuatu yang diwajibkan (oleh undang-undang)”.

Penentuan apakah suatu perbuatan merupakan tindak pidana, maka perbuatan tersebut harus diatur dalam undang-undang pidana. Undang-undang pidana tersebut harus memuat unsur-unsur yang menjadi ciri atau sifat perbuatan tersebut, sehingga dapat dibedakan dari perbuatan lain yang tidak dilarang. Tindak pidana adalah perbuatan yang dilarang oleh undang-undang pidana dan dikenai sanksi pidana. Sanksi pidana tersebut merupakan ciri atau sifat yang membedakan tindak pidana dari perbuatan lain yang tidak dilarang.⁹

Seluruh perilaku pidana yang ada di Kitab Undang-Undang Hukum Pidana secara umum bisa dijabarkan pada unsur-unsur yang ada sejatinya dibagi dalam 2 macam unsur, yaitu unsur subjektif dan objektif. pada dasarnya dapat kita bagi menjadi dua macam unsur, yakni unsur-unsur subjektif dan unsur-unsur objektif. Unsur subjektif ialah unsur yang melakukan kepada diri pelaku maupun berkaitan dengan diri pelaku, dan termasuk didalamnya yakni semua yang terkandung di dalam hatinya. Sedang unsur objektif sendiri ialah unsur

⁹ Suyanto, *Pengantar Hukum Pidana*, 74.

yang berkaitan dengan kondisi yakni di saat kondisi yang mana perilaku si pelaku ini wajib dilaksanakan. Unsur subyektif dari sebuah tindak pidana ialah:

- a. Kesengajaan atau tidak kesengajaan (*doulus* atau *culpa*);
 - b. Maksud atau *voornemen* dalam sebuah percobaan atau *poging* layaknya yang tercantum dalam pasal 53 ayat (1) KUHP;
 - c. Berbagai macam maksud atau *oogmerk* seperti yang ada contohnya pada kejahatan mencuri, menipu, memeras, memalsukan dan sebagainya;
 - d. Membuat rencana dulu atau *voorbedachte raad* contohnya yang ada dalam kejahatan membunuh berdasarkan Pasal 340 KUHP;
 - e. Rasa takut atau *vress* misalnya yang antara lain ada pada rumusan tindak pidana dalam Pasal 308 KUHP.
- Unsur objektif sebuah tindak pidana ialah:

- a) Sifat melanggar hukum atau *wederrechtelijkheid*;
- b) Kualitas pelaku, contohnya “Keadaan sebagai seorang pegawai negeri” pada kejahatan jabatan berdasarkan Pasal 415 KUHP atau “keadaan sebagai pengurus atau komisaris dari suatu perseroan terbatas” pada kejahatan berdasarkan Pasal 398 KUHP. Kausalitas, yaitu korelasi dari sebuah tindakan sebagai penyebab dengan sebuah kenyataan sebagai akibat.¹⁰

¹⁰ P.A.F. Lamintang and Franciscus Theojunior Lamintang, *Dasar-Dasar Hukum Pidana Di Indonesia*, 2nd ed. (Jakarta: Sinar Grafika, 2016), 191-193.

Menurut Moeljatno, tindak pidana adalah perbuatan yang dilarang oleh undang-undang dan diancam dengan hukuman. Tindak pidana terdiri dari dua unsur, yaitu unsur formal dan unsur materiil:

a. Unsur Formal adalah unsur yang menentukan apakah suatu perbuatan merupakan tindak pidana atau tidak. Unsur formal ini terdiri dari dua unsur lagi, yaitu:

1) Perbuatan

Perbuatan adalah tindakan atau perbuatan yang dilakukan oleh manusia. Perbuatan ini dapat berupa perbuatan aktif, yaitu perbuatan yang menimbulkan akibat tertentu, atau perbuatan pasif, yaitu perbuatan yang tidak melakukan sesuatu yang seharusnya dilakukan.

2) Larangan

Larangan adalah perbuatan yang diatur dalam undang-undang dan diancam dengan hukuman. Undang-undang yang mengatur larangan ini dapat berupa undang-undang pidana, undang-undang perdata, atau undang-undang lainnya.

b. Unsur Materiil adalah Unsur yang menentukan apakah suatu perbuatan merupakan tindak pidana yang bersifat melawan hukum atau tidak. Unsur ini terdiri dari dua unsur yaitu :

1) Melawan Hukum

Melawan hukum adalah perbuatan yang bertentangan dengan peraturan perundang-undangan. Peraturan perundang-undangan yang dimaksud adalah undang-undang, peraturan pemerintah, peraturan daerah, dan peraturan lainnya yang bersifat mengikat secara umum.

2) Akibat

Akibat adalah akibat yang ditimbulkan oleh perbuatan tersebut. Akibat ini dapat berupa akibat yang bersifat materiil, yaitu akibat yang dapat diukur secara fisik, atau akibat yang bersifat non materiil, yaitu akibat yang tidak dapat diukur secara fisik.

Selain unsur formal dan materiil, Moeljanto juga membagi unsur-unsur tindak pidana menjadi dua kategori, yaitu unsur subjektif dan unsur subjektif.¹¹

a. Unsur subjektif adalah unsur yang berkaitan dengan diri orang yang melakukan perbuatan. Unsur subjektif ini terdiri dari unsur-unsur yang bersifat personal, seperti misalnya unsur pegawai negeri dalam tindak pidana korupsi.

¹¹ Effendi, Jonaedi. *Cepat & Mudah Memahami Hukum Pidana*, 40.

- b. Unsur objektif adalah unsur yang berkaitan dengan keadaan di luar diri orang yang melakukan perbuatan. Unsur objektif ini terdiri dari unsur unsur yang bersifat non personal, seperti misalnya unsur penghasutan di muka umum dalam tindak pidana penghasutan.

3. Jenis-jenis Tindak Pidana

Tindak pidana merupakan perbuatan yang dilarang oleh hukum dan diancam dengan sanksi pidana. Jenis-jenis tindak pidana dapat dibedakan berdasarkan berbagai kriteria, salah satunya berdasarkan unsur-unsurnya. Unsur-unsur tindak pidana merupakan unsur-unsur yang harus terpenuhi agar suatu perbuatan dapat dikategorikan sebagai tindak pidana. Pembagian tindak pidana berdasarkan unsur-unsurnya dapat dilakukan dengan berbagai cara. Salah satu cara pembagian tersebut adalah berdasarkan berat ringannya kejahatan. Pada awalnya, ahli hukum membagi tindak pidana berdasarkan tingkat berat ringannya, yaitu:

- a. *Crimines atrocissima*, yaitu tindak pidana yang sangat berat, misalnya pembunuhan berencana.
- b. *Crimines atrocia*, yaitu tindak pidana yang berat, misalnya penganiayaan berat.
- c. *Crimines levia*, yaitu tindak pidana ringan, misalnya pencurian ringan.

Pembagian ini tidak didasarkan pada suatu asas tertentu, melainkan hanya berdasarkan tingkat berat

ringannya kejahatan. Berat ringannya kejahatan ditentukan berdasarkan peraturan hukum yang mengaturnya.¹² KUHP mengadakan pembagian ke dalam (2) jenis tindak pidana yaitu sebagai berikut:¹³

a. Kejahatan (*misdrijven*);

Kejahatan adalah perbuatan-perbuatan optimum yang dianggap telah mengandung sifat ketidakadilan dan berdasarkan sifat itu supaya perbuatan yang demikian itu sudah patut dilarang dan diancam hukuman. Sungguhpun perbuatan itu belum dilarang dan diancam dengan hukum oleh UU, toh perbuatan itu sudah patut dihukum. contoh: Pembunuhan, pencurian, penipuan, dan lain lain.

b. Pelanggaran (*overtredingen*);

Pelanggaran adalah perbuatan-perbuatan yang hanya dapat dihukum oleh karena dilarang oleh UU (*die hen strafwaardigheid ontle nen aan de wet*). Contoh: dilarang membuang sampah sembarangan, dan lain lain.

Tindak pidana merupakan perbuatan yang dilarang oleh hukum dan diancam dengan sanksi pidana. Tindak pidana dapat dibedakan berdasarkan cara merumuskannya, yaitu menjadi delik formal dan delik material:

¹² Achmad Zaeni Dachlan, *Analisis Hukum Pidana Islam Dan HAM Terhadap Hak Korban Dan Saksi Dalam Undang-Undang Nomor 12 Tahun 2022 Tentang Tindak Pidana Kekerasan Seksual*, skripsi Universitas Islam Negeri Walisongo, Semarang 2022, 40-41.

¹³ Rasyid Ariman dan Fahmi Raghieb, *Hukum Pidana*, (Malang, Setara Press, 2015), 72.

- a. Delik Formal, adalah tindak pidana yang perumusannya menitikberatkan pada perbuatan yang dilarang. Tindak pidana ini dianggap telah selesai dengan telah dilakukannya perbuatan yang dilarang, tanpa mempersoalkan akibatnya, contoh: Pencurian (Pasal 362 KUHP), Penghasutan (Pasal 160 KUHP).
- b. Delik Materiil, adalah tindak pidana yang perumusannya menitikberatkan pada akibat yang dilarang. Tindak pidana ini dianggap telah selesai apabila akibat yang dilarang telah terjadi, contoh: Pembunuhan (Pasal 338 KUHP), Penipuan (Pasal 378 KUHP).

Perbedaan antara delik formal dan delik material terletak pada penitikberatan perumusannya. Delik formal menitikberatkan pada perbuatan yang dilarang, sedangkan delik material menitikberatkan pada akibat yang dilarang.¹⁴ Sementara menurut jenisnya, delik dibedakan atas:¹⁵

- a. Delik aduan, yaitu tindak pidana yang hanya dapat dituntut atas dasar pengaduan dari orang yang merasa dirugikan atau dirugikan oleh perbuatan itu, berdasarkan KUHP, delik aduan dibedakan menjadi dua jenis, yaitu:
 - 1) Delik Aduan Murni, yang hanya dapat dituntut atas dasar pengaduan dari korban atau orang yang menderita akibat adanya peristiwa

¹⁴ Mahrus Ali, *Dasar Dasar Hukum Pidana*, (Jakarta Sinar Grafika, 2011), 102.

¹⁵ Tofik Yanuar, *Hukum Pidana*, (Jakarta, PT Sangir Multi Usaha, 2022), 49-50.

pidana itu. Pengaduan dalam delik aduan murni bersifat mutlak, artinya tanpa adanya pengaduan dari korban atau orang yang menderita, maka tindak pidana tersebut tidak dapat dituntut, contoh: Pencemaran nama baik (Pasal 310 KUHP), Penganiayaan ringan (Pasal 352 KUHP).

- 2) Delik Aduan Relatif, yang dapat dituntut atas dasar pengaduan dari korban atau orang yang menderita akibat adanya peristiwa pidana itu, tetapi juga dapat dituntut oleh jaksa tanpa adanya pengaduan dari korban. Pengaduan dalam delik aduan relatif bersifat fakultatif, artinya pengaduan dari korban atau orang yang menderita tidak diperlukan, tetapi pengaduan tersebut dapat diberikan, contoh: Pelecehan seksual (Pasal 289 KUHP), Pemerkosaan (Pasal 285 KUHP).
- b. Delik *Comissionis*, yaitu delik yang berupa pelanggaran terhadap larangan, adalah berbuat sesuatu yang dilarang, misalnya melakukan pencurian, pembunuhan dan penipuan.
- c. Delik *Omissionis*, yaitu delik yang berupa pelanggaran terhadap perintah, adalah tidak melakukan sesuatu yang diperintahkan/yang diharuskan, misal: Tidak menghadap sebagai saksi di muka pengadilan (Pasal 522).
- d. Delik *Comissionis per ommissionis comissa*, yaitu delik yang berupa pelanggaran larangan (*dus delik comissionis*), akan tetapi dapat dilakukan dengan cara tidak berbuat, misal: seorang ibu yang

membunuh anaknya dengan tidak memberi air susu (Pasal 338, 340 KUHP), seorang penjaga wissel yang menyebabkan kecelakaan kereta api dengan sengaja tidak memindahkan wissel (Pasal 194 KUHP).¹⁶

Tindak pidana dapat dibedakan atas dasar-dasar tertentu, yaitu sebagai berikut:¹⁷

- a. Menurut sistem KUHP, dibedakan antara kejahatan (*misdrijven*) dimuat dalam buku II dan pelanggaran (*overtredingen*) dimuat dalam buku III;
- b. Menurut cara merumuskannya, dibedakan antara tindak pidana formil (*formeel delicten*) dan tindak pidana materiil (*materieel delicten*);
- c. Berdasarkan bentuk kesalahannya, dibedakan antara tindak pidana sengaja (*doleus delicten*) tindak pidana tidak dengan sengaja (*culpose delicten*);
- d. Berdasarkan macam perbuatannya, dapat dibedakan antara tindak pidana aktif/positif dapat juga disebut tindak pidana komisi (*delicta commissionis*) dan tindak pidana pasif/negatif, disebut juga tindak pidana omisi (*delicta omissionis*);
- e. Berdasarkan saat dan jangka waktu terjadinya, maka dapat dibedakan antara tindak pidana terjadi seketika dan tindak pidana terjadi dalam waktu

¹⁶ Effendi, Jonaedi. *Cepat & Mudah Memahami Hukum Pidana*, 46.

¹⁷ Adami Chazawi, 2005, *Pelajaran Hukum Pidana Bagian 1*, (Jakarta, PT Raja Grafindo, 2005) 121-122.

lama atau berlangsung lama atau berlangsung terus;

- f. Berdasarkan sumbernya, dapat dibedakan antara tindak pidana umum dan tindak pidana khusus;
- g. Dilihat dari sudut subjek hukumnya, dapat dibedakan antara tindak pidana *communia* (*delicta communia*, yang dapat dilakukan oleh siapa saja), dan tindak pidana *propria* (dapat dilakukan hanya oleh orang memiliki kualitas pribadi tertentu);
- h. Berdasarkan perlu tidaknya pengaduan dalam hal penuntutan, maka dapat dibedakan antara tindak pidana biasa (*gewone delicten*) dan tindak pidana aduan (*klachtdelicten*);
- i. Berdasarkan berat-ringannya pidana yang diancamkan, maka dapat dibedakan antara tindak pidana bentuk pokok (*eenvoudige delicten*), tindak pidana yang diperberat (*gequalificeerde delicten*) dan tindak pidana yang diperingan (*gepriviligieerde delicten*);
- j. Berdasarkan kepentingan hukum yang dilindungi, maka tindak pidana tidak terbatas macamnya bergantung dari kepentingan hukum yang dilindungi, seperti tindak pidana terhadap nyawa dan tubuh, terhadap harta benda, tindak pidana pemalsuan, tindak pidana terhadap nama baik, terhadap kesusilaan dan lain sebagainya;
- k. Dari sudut berapa kali perbuatan untuk menjadi suatu larangan, dibedakan antara tindak pidana tunggal (*enkelvoudige delicten*) dan tindak pidana berangkai (*samengestelde delicten*).

B. Kejahatan Dunia Maya (*CyberCrime*)

1. Pengertian

Secara Terminologis, kejahatan di bidang teknologi informasi dengan basis komputer sebagaimana terjadi saat ini, dapat disebut dengan beberapa istilah yaitu *computer missue*, *computer abuse*, *computer fraud*, *computer related crime*, *computer-assisted crime*, atau *computer crime*.¹⁸ Istilah kejahatan yang berhubungan dengan komputer (*computer-related crime*) seringkali digunakan Perserikatan Bangsa Bangsa (PBB) dalam dokumen dokumennya. Namun demikian, konvensi internasional pada tahun 2001 tentang pengaturan kejahatan yang berhubungan dengan komputer dan pemberantasannya menggunakan istilah *cybercrime*, sehingga konvensinya berjudul *Convention on Cybercrime*. Barda Nawawi Arief mengemukakan bahwa pengertian kejahatan yang berhubungan dengan komputer (*computer-related crime*) sama dengan *cybercrime*¹⁹.

Sebagai bukti tentang penggunaan istilah kejahatan yang berhubungan dengan komputer oleh PBB, dalam Laporan Dokumen Kongres PBB ke-10 di Wina, tanggal 19 Juli 2000 menggunakan istilah *computer-related crime*, kemudian mengatur dua bentuk berikut:

¹⁸ Widodo, *Aspek Hukum Pidana Kejahatan Mayantara*, (Yogyakarta, Aswaja, 2013), 5

¹⁹ Barda Nawawi Arief, *Perbandingan Hukum Pidana*, (Jakarta, PT Raja Grafindo Persada, 2002), 259.

“The term “computer-related crime” had been developed encompass both the entirely new forms of crime that were directed at computer, networks and their users, and the more traditional form of crime that were now being committed with the use or assistance of computer equipment”.....

- a. *Cybercrime in narrow sense (computer crime); any illegal behavior directed by means of electronic operations that targets the security of computer system and the data processed by them.*
- b. *Cybercrime in broader sense (computer-related crime); any illegal behavior committed by means of, or in relation to, a computer system network, including such crimes as illegal possession, offering or distributing information by means of computer system on network.²⁰*

Kejahatan siber (*Cyber crime*) dapat didefinisikan sebagai perbuatan melawan hukum yang merugikan dan dapat menimbulkan kerugian yang signifikan jika tidak segera ditangani. Perbuatan ini dilakukan dengan memanfaatkan kecanggihan komputer dan bidang informatika, terutama komputer dan internet. kejahatan siber merupakan perbuatan yang sangat berbahaya dan telah diancam dengan sanksi hukum di berbagai negara di dunia.

Cybercrime adalah tindak pidana kriminal yang dilakukan pada teknologi internet (*Cyber Space*), baik yang menyerang fasilitas umum maupun kepemilikan pribadi. Secara teknik dapat dibedakan menjadi

²⁰ Agus Rahardjo, *Cybercrime: Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*, (Bandung, PT Citra Aditya Bakti, 2002), 67.

offline crime, *semi online crime* dan *cybercrime*. Contoh dari *offline crime* adalah dengan cara yang sederhana misal mencuri dompet seseorang untuk kemudian diambil kartu kreditnya, atau bekerja sama dengan kasir untuk mencatat nomor kartu kredit tersebut yang kemudian menduplikatnya. Contoh teknik *semi online crime* adalah memasang *skimming* (pencurian informasi kartu kredit/debit secara ilegal) di mesin ATM untuk mencuri informasi kartu debit korban. Sedangkan untuk *cybercrime* orang pelaku dan korban tidak perlu bertatap muka, dan bersentuhan, yaitu dengan menggunakan teknologi yang canggih, seperti penggunaan situs palsu klik BCA, mengirim surat undangan pernikahan ke nomor whatsapp korban, yang dimana ketika kita klik mengunduh surat undangan tersebut maka handphone yang digunakan oleh korban tersedot saldo rekening bank maupun aplikasi pembayaran online lainnya, dan lain lain. Masing-masing teknik memiliki karakteristik tersendiri, namun perbedaan utama diantar ketiganya adalah keterhubungan dengan jaringan informasi publik (internet).²¹

2. Jenis-jenis

Meskipun kejahatan di dunia maya telah menjadi hal yang umum karena banyaknya korban, hukum yang berlaku di Indonesia masih belum dapat menyelesaikan kasus-kasus ini secara menyeluruh. Hal ini sangat merugikan banyak pihak, sehingga peran jaksa yang memiliki pemahaman, pemikiran,

²¹ Yurizal, *Penegakkan Hukum Tindak Pidana Cyber Crime*, (Malang, Media Nusa Creative, 2018), 16-17.

dan cara pandang yang luas, serta didukung oleh ilmu dan wawasan yang tinggi mengenai teknologi informasi, menjadi sangat penting. Dengan demikian, hal-hal yang mendorong maraknya kejahatan dunia maya dapat dihilangkan, dan faktor-faktor yang melatarbelakangi timbulnya kasus kejahatan dunia maya di kalangan masyarakat saat ini dapat diketahui.

Selain itu, perlu adanya hukuman yang tegas dan berkualitas. Faktanya, masih ditemukan hakim yang belum menguasai teknologi informasi dan pengetahuan mengenai hal tersebut masih sangat minim. Seharusnya, dengan perkembangan teknologi yang semakin pesat, para hakim juga perlu meningkatkan wawasan mereka mengenai teknologi tersebut agar terhindar dari penyalahgunaan.

Dari kegiatan yang dilakukan untuk bertindak kejahatan, terdapat pembagian jenis aktivitas *cybercrime* diantaranya berikut ini:

a. *Cybercrime* sebagai tindakan murni kriminal

Ketika kejahatan ini dilatarbelakangi oleh motif tindakan kriminalitas maka sering disebut dengan kejahatan murni, di mana dalam melakukan perbuatan tersebut dibantu dengan internet yang dijadikan sebagai jalan atau media. Misalkan *Carding*, jenis ini dilakukan dengan cara mencuri atau mengambil nomor kartu kredit orang lain yang nantinya akan dimanfaatkan sebagai pembayaran transaksi online di internet. Selain itu, menggunakan media lain seperti webserver dan mailing list yang dipakai dalam menyebarkan material bajakan. Hal ini diawali dengan orang yang

tidak dikenal atau anonym yang melakukan pengiriman email dengan isi di dalamnya meneror berbagai promosi atau meminta bantuan. Kedua hal tersebut juga dapat dikategorikan sebagai kejahatan yang menjadikan media internet ini sebagai sarana. Kebanyakan pada negara maju telah menegaskan hukum dari para pelaku spam tersebut dikarenakan perbuatan itu sudah termasuk dalam melanggar privasi dan dapat mengganggu atau mengusik kehidupan seseorang.

b. *Cybercrime* sebagai kejahatan abu abu

Dalam bentuk kejahatan jenis ini masih susah untuk ditentukan dan dikategorikan apakah telah masuk dalam tindakan kriminal atau bukan dikarenakan motif yang digunakan terkadang tidak dilakukan untuk hal yang jahat. Contohnya yaitu *probing*. Dimana dikenal dengan suatu kegiatan yang mengintai sistem orang lain dan langkah yang dilakukan adalah melakukan pengumpulan informasi sebanyak yang bisa dikumpulkan yang diambil dari pencurian sistem tersebut. Dan hal yang diintai ini seperti port-port yang ada baik yang terbuka maupun tertutup dan sistem operasi yang dipakai. Jika dilihat melalui sasaran nya, maka perbuatan *cybercrime* terbagi menjadi berbagai jenis yaitu:

1) *Cybercrime* yang menyerang individu (*Againts Person*)

Sasaran yang dituju dalam kejahatan ini adalah perorangan. Namun tidak sembarang tiap individu saja tetapi telah disesuaikan

dengan kriteria yang ditentukan oleh si penyerang selaras dengan tujuan dilakukan tindak kejahatan pada orang tersebut.

- 2) *Cyber crime* menyerang hak milik (*Againts Property*)

Alasan tindak kejahatan jenis ini digunakan dalam mengganggu hak milik orang lain. Terdapat beberapa contoh di antaranya melakukan akses dalam komputer dengan tanpa izin dan secara tidak sah atau illegal melalui dunia *cyber*, *carding*, *hijacking* dan masih banyak lainnya untuk tujuan membuat rugi kepemilikan orang tersebut.

- 3) *Cybercrime* yang menyerang pemerintah (*Againts Government*)

Berbeda dengan di atas yang menyerang perorangan, jenis ini sasarannya diberikan kepada pemerintah dengan tujuan tertentu. Hal yang dilakukan oleh pelaku *cybercrime* dengan melakukan peneroran dan pengancaman kepada pemerintah. Tidak hanya menteror, kegiatan ini juga melakukan cracking ke situs resmi pemerintah ataupun militer.²²

Kejahatan yang berhubungan erat dengan penggunaan teknologi yang berbasis komputer dan jaringan telekomunikasi dalam beberapa literatur dan praktiknya dikelompokkan dalam beberapa bentuk, antara lain:²³

²² Tanhella,dkk., *Buku Ajar Etika Hukum Cyber*, (Magetan, CV AE MEDIA GRAFIKA,2021), 85-87.

²³ Maksun, *Kejahatan Siber (Cyber Crime)Suatu Pengantar*,(Jakarta, Kencana, 2013), 51-54.

- a. *Defacing*, yaitu kejahatan dunia maya yang paling favorit karena hasil kejahatannya dapat langsung dilihat oleh masyarakat. Kejahatan ini dilakukan dengan mengubah tampilan sesuai keinginan pelaku kejahatan sehingga bisa saja menampilkan tulisan-tulisan provocative atau gambar lucu.²⁴
- b. *Unauthorized access to computer system and service*, yaitu kejahatan yang dilakukan dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin, atau tanpa pengetahuan dari pemilik sistem jaringan komputer yang dimasukinya. Biasanya pelaku kejahatan (*hacker*) melakukannya dengan maksud sabotase ataupun pencurian informasi penting dan rahasia. Namun, ada juga yang melakukannya hanya karena merasa tertantang untuk mencoba keahliannya menembus suatu sistem yang memiliki tingkat proteksi tinggi. Kejahatan ini semakin marak dengan berkembangnya teknologi internet.
- c. *Illegal contents*, yaitu kejahatan dengan memasukkan data atau informasi ke internet tentang sesuatu hal yang tidak benar, tidak etis, dan dianggap melanggar hukum atau mengganggu ketertiban umum.
- d. *Data forgery*, yaitu kejahatan dengan memalsukan data pada dokumendokumen penting yang tersimpan sebagai scrptless

²⁴ Budi Sahariyanto, *Tindak Pidana Teknologi Informasi (Cyber Crime) Urgensi Pengaturan dan Celah Hukumnya*, (Jakarta: Rajawali Pers, 2012).

document melalui internet. Kejahatan ini biasanya ditujukan pada dokumen-dokumen *e-commerce* dengan membuat seolah-olah terjadi “salah ketik” yang pada akhirnya akan menguntungkan pelaku.

- e. *Cyber espionage*, yaitu kejahatan yang 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 atau data-data pentingnya tersimpan dalam suatu sistem komputerisasi.
- f. *Cyber sabotage and extortion*, yaitu kejahatan yang dilakukan dengan membuat gangguan, perusakan, atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang tersambung dengan internet.
- g. *Offence against intellectual property*, yaitu kekayaan yang ditujukan terhadap hak kekayaan intelektual yang dimiliki seseorang di internet. Contohnya peniruan tampilan web page suatu situs milik orang lain secara ilegal.
- h. *Infringements of privacy*, yaitu kejahatan yang ditujukan terhadap informasi seseorang yang merupakan hal yang sangat pribadi dan rahasia.

C. Sistem Elektronik

1. Pengertian

Sistem elektronik menurut Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Elektronik dan Transaksi Elektronik, pada pasal 1 ayat (5) adalah:

“Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan Informasi Elektronik.”²⁵

UU ITE juga memberikan dasar hukum mengenai kekuatan hukum alat bukti elektronik dan syarat formil dan materil alat bukti elektronik agar dapat diterima di persidangan. Alat bukti elektronik ialah informasi elektronik dan/atau dokumen elektronik yang memenuhi persyaratan formil dan persyaratan materil yang diatur dalam UU ITE. Informasi elektronik dan/atau dokumen elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah. Sistem elektronik juga terkait dengan *cyber law*. *Cyber law* sendiri terdiri dari dua bagian, yaitu hukum publik dan hukum privat. Pada hukum publik, terdapat yuridiksi, etika kegiatan online, perlindungan konsumen, anti monopoli, persaingan sehat, perpajakan, *regulatory*

²⁵ Undang Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.

body, *data protection*, dan *cybercrimes*. Sedangkan pada hukum privat, terdapat hak kekayaan intelektual (HAKI), e-commerce, electronic contract, domain name, dan insurance.

Sistem Elektronik adalah interkoneksi fisik komponen, atau bagian, yang mengumpulkan berbagai jumlah informasi secara bersamaan. Ini dilakukan dengan bantuan perangkat input seperti sensor, yang merespon dengan cara tertentu terhadap informasi ini dan kemudian menggunakan energi listrik dalam bentuk aksi keluaran untuk mengontrol proses fisik atau melakukan beberapa jenis operasi matematika pada sinyal. Sistem elektronik adalah sekumpulan perangkat dan prosedur elektronik yang berfungsi untuk mengelola informasi elektronik.²⁶

Sistem elektronik adalah suatu rangkaian atau jaringan komponen elektronik yang bekerja bersama untuk mencapai tujuan tertentu. Sistem ini menggunakan prinsip-prinsip elektronika untuk memproses, mentransmisikan, atau menyimpan informasi. Komponen-komponen elektronik dalam sistem ini dapat berupa transistor, resistor, kapasitor, IC (*Integrated Circuit*), mikrokontroler, sensor, dan berbagai elemen elektronik lainnya.

Sistem elektronik yang terpenting dapat memiliki berbagai aplikasi dan kompleksitas, mulai dari perangkat elektronik konsumen seperti telepon pintar dan komputer pribadi hingga sistem yang digunakan dalam industri atau militer. Beberapa contoh sistem

²⁶ UU 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik.

elektronik termasuk sistem komputer, sistem kendali otomatis, sistem komunikasi, dan banyak lagi.

2. **Jenis-jenis Sistem Elektronik**

Sistem elektronik adalah sistem yang menggunakan komponen-komponen elektronik untuk mengolah, mengendalikan, atau mengubah sinyal-sinyal listrik. Sistem elektronik dapat dibedakan menjadi beberapa jenis berdasarkan fungsi, sinyal, dan komponen yang digunakan. Berikut adalah beberapa jenis sistem elektronik yang umum²⁷:

- a. Sistem elektronik analog: sistem yang menggunakan sinyal listrik yang bervariasi secara kontinu dan memiliki hubungan proporsional dengan besaran fisik yang diukur atau dikendalikan. Contoh sistem elektronik analog adalah amplifier audio, osiloskop, dan radio FM.
- b. Sistem elektronik digital: sistem yang menggunakan sinyal listrik yang hanya memiliki dua nilai, yaitu 0 dan 1, yang disebut sebagai bit. Sinyal digital dapat merepresentasikan data, informasi, atau instruksi dalam bentuk kode biner. Contoh sistem elektronik digital adalah komputer, kalkulator, dan jam digital¹.
- c. Sistem elektronik hibrid: sistem yang menggabungkan sistem elektronik analog dan digital untuk memanfaatkan kelebihan masing-masing sistem. Contoh sistem elektronik hibrid adalah telepon seluler, kamera digital, dan modem.

²⁷ Tere, *Pengertian Sistem Komunikasi: Komponen, Fungsi, dan Jenis-Jenisnya*. (Gramedia Blog, 2020).

- d. Sistem elektronik komunikasi: sistem yang menggunakan sinyal listrik untuk mengirim atau menerima informasi antara dua atau lebih titik. Sistem elektronik komunikasi dapat menggunakan media transmisi yang berbeda, seperti kabel, gelombang radio, gelombang mikro, atau satelit. Contoh sistem elektronik komunikasi adalah telepon, televisi, radio, dan internet.
- e. Sistem elektronik pembayaran: sistem yang menggunakan teknologi elektronik untuk melakukan transaksi keuangan secara cepat, mudah, dan aman. Sistem elektronik pembayaran dapat menggunakan berbagai alat atau metode, seperti kartu perbankan, dompet digital, terminal POS, atau internet banking⁴.

Berikut jenis-jenis dari sistem elektronik berdasarkan kegunaannya adalah:

- a. Sistem Mikroelektronika:
Mungkin melibatkan pengembangan dan integrasi sirkuit mikroelektronika ke dalam berbagai aplikasi, seperti sistem komputer, sensor, atau perangkat konsumen.
- b. Sistem Komunikasi Nirkabel:
Penelitian tentang protokol komunikasi nirkabel, pengembangan teknologi 5G atau yang lebih baru, dan aspek-aspek keamanan dalam sistem komunikasi.
- c. Sistem Kontrol Otomatis:
Fokus pada pengembangan algoritma kontrol otomatis, implementasi sistem kontrol dalam

industri, dan pemantauan otomatis berbagai proses.

- d. Sistem Elektronik Medis:
Mungkin membahas pengembangan peralatan medis baru, perangkat diagnosis, atau sistem pemantauan pasien.
- e. Sistem Sensor dan Pemantauan:
Penelitian terkait pengembangan sensor terbaru, penggunaan teknologi sensor dalam berbagai konteks, dan pengintegrasian sensor dalam sistem pemantauan.
- f. Sistem Keamanan Elektronik:
Melibatkan penelitian tentang teknologi keamanan terbaru, analisis keamanan sistem, dan pengembangan perangkat keamanan elektronik.
- g. Sistem Elektronik Energi:
Membahas pengembangan teknologi untuk efisiensi energi, penyimpanan energi, atau sistem elektronik dalam konteks energi terbarukan.
- h. Sistem Elektronik Pembelajaran (*E-Learning*):
Fokus pada integrasi teknologi dalam pendidikan, pengembangan platform e-learning, atau evaluasi efektivitas sistem e-learning.
- i. Sistem Elektronik Pemrosesan Sinyal:
Melibatkan penelitian tentang algoritma pemrosesan sinyal digital, implementasi

perangkat lunak, atau aplikasi dalam pemrosesan suara, gambar, atau video.

- j. Sistem Elektronik Kendaraan Otonom:
Mungkin membahas teknologi kendaraan otonom, sistem pengenalan lingkungan, dan integrasi sistem elektronik dalam kendaraan tanpa pengemudi.

3. Ancaman dan Serangan yang Mengakibatkan Terganggunya Sistem Elektronik

Dalam era digital seperti saat ini, sistem elektronik memainkan peran yang semakin penting dalam kehidupan manusia. Sistem elektronik digunakan dalam berbagai bidang, mulai dari industri, pemerintahan, hingga kehidupan sehari-hari. Namun, penggunaan sistem elektronik juga menimbulkan berbagai ancaman dan serangan yang dapat mengganggu sistem tersebut.

Ancaman dan serangan terhadap sistem elektronik dapat diklasifikasikan menjadi dua, yaitu ancaman fisik dan ancaman non-fisik. Ancaman fisik adalah ancaman yang berasal dari faktor fisik, seperti kerusakan perangkat keras, gangguan aliran listrik, atau bencana alam. Ancaman non-fisik adalah ancaman yang berasal dari faktor non-fisik, seperti serangan malware, serangan *denial-of-service* (DoS), atau serangan pencurian data. Ancaman dan serangan terhadap sistem elektronik dapat menimbulkan berbagai kerugian, mulai dari kerugian finansial, kerugian reputasi, hingga kerugian korban jiwa. Oleh karena itu, penting untuk memahami berbagai

ancaman dan serangan terhadap sistem elektronik agar dapat diantisipasi dan dimitigasi.

a. Ancaman Yang Mengakibatkan Terganggunya Sistem Elektronik

1) Sumber Ancaman

Sumber Ancaman adalah entitas yang berkeinginan atau memiliki niat dan benar-benar secara nyata akan melakukan kegiatan yang melanggar norma dan hukum, aturan dan ketentuan serta kaidah atau kontrol keamanan informasi serta aset fisik lainnya, dengan tujuan untuk mendapatkan keuntungan yang bersifat materil dan immateril. Ancaman dan serangan tersebut dapat dilakukan oleh pelaku yang mewakili pemerintah (*State Actor*) atau non pemerintah (*Non State Actor*), sehingga pelaku bisa bersifat perorangan, kelompok, golongan, organisasi atau bahkan sebuah negara. Secara umum unsur-unsur yang dapat diidentifikasi memiliki potensi sebagai sumber ancaman terdiri atas :

- a) Sumber internal dan eksternal;
- b) Kegiatan Intelejen;
- c) Kekecewaan
- d) Investigasi;
- e) Organisasi Eksremis;
- f) *Hactivists*;
- g) Grup kejahatan yang terorganisir;
- h) Persaingan, permusuhan dan konflik;
- i) Teknologi.

2) Aspek Ancaman

Aspek ancaman adalah segala sesuatu yang melatarbelakangi terjadinya ancaman dan serangan siber, yang meliputi aspek-aspek Ideologi, Politik, Ekonomi, Sosial, Budaya, Kebangsaan, Militer, Ilmu Pengetahuan dan Teknologi serta aspek lain yang terkait dalam kehidupan berbangsa, bernegara dan bermasyarakat termasuk kepentingan pribadi.

3) Bentuk Ancaman

Bentuk ancaman siber yang sering terjadi saat ini dapat berupa hal-hal sebagai berikut :

- a) Serangan *Advanced Persistent Threats (APT)*, *Denial of Service (DoS)* dan *Distributed Denial of Service (DDoS)*, biasanya dilakukan dengan melakukan *overloading* kapasitas sistem dan mencegah pengguna yang sah untuk mengakses dan menggunakan sistem atau sumber daya yang ditargetkan. Serangan ini bertujuan untuk mengganggu operasional sistem, dengan cara menghadapkan sistem pada permintaan akses dan proses yang jauh lebih besar dari yang bisa ditangani sistem. Sehingga sistem menjadi terlalu sibuk dan crash, akibatnya menjadi tidak dapat melayani atau tidak dapat beroperasi. Permasalahan ini merupakan ancaman yang berbahaya bagi organisasi yang mengandalkan hampir sepenuhnya pada kemampuan

internet guna menjalankan roda kegiatannya.

- b) Serangan *Defacement*, dilakukan dengan cara melakukan penggantian atau modifikasi terhadap halaman web korban sehingga isi dari halaman web korban berubah sesuai dengan motif penyerang.
- c) Serangan *Phishing*, dilakukan dengan cara memberikan alamat *website* palsu dengan tampilan persis sama dengan *website* aslinya. Tujuan dari serangan phishing ini adalah untuk mendapatkan informasi penting dan sensitif seperti *username*, *password* dan lain-lain.
- d) Serangan *Malware*, yaitu suatu program atau kode berbahaya yang dapat digunakan untuk mengganggu operasi normal dari sebuah sistem komputer. Biasanya program malware telah dirancang untuk mendapatkan keuntungan finansial atau keuntungan lain yang direncanakan. Jumlah serangan malware terus berkembang, sehingga saat ini telah menjadi pandemi yang sangat nyata. *Malware* telah terjadi dimana-mana dan mempengaruhi semua orang yang terlibat dalam setiap sektor kegiatan. Istilah virus generik digunakan untuk merujuk setiap program komputer berbahaya yang mampu mereproduksi dan menyebarkan dirinya sendiri.

- e) Penyusupan siber, yang dapat menyerang sistem melalui identifikasi pengguna yang sah dan parameter koneksi seperti *password*, melalui eksploitasi kerentanan yang ada pada sistem. Metode utama yang digunakan untuk mendapatkan akses ke dalam sistem adalah :
- Menebak. Sandi Sandi yang begitu jelas, seperti nama pengguna, nama pasangan atau anak, tanggal lahir atau berbagai hal yang penting yang berkaitan dengan diri dan keluarganya, sangat mudah untuk ditebak dan dipecahkan.
 - *Account* yang tidak terlindungi. Pengguna juga dapat melakukan kesalahan, dengan tidak memasang *password* atau dengan mudah memberikan *password* kepada orang lain.
 - Penipuan dan Rekayasa Sosial, misalnya pelaku dapat mengaku dan bertindak sebagai *administrator* dan meminta *password* dengan beberapa alasan teknis. Dalam sejumlah besar kasus, pengguna akan mengungkapkan data mereka. Pelaku dapat menipu melalui telepon atau pesan elektronik. Beberapa orang pelaku tidak faham komputer, tetapi ternyata pelaku dapat memperoleh

kunci sesuai dengan sistem yang mereka inginkan untuk ditembus.

- Mendengarkan lalu lintas komunikasi data. Penyadap akan mendengarkan data yang tidak terenkripsi yang dikirimkan melalui jaringan melalui protokol komunikasi. Mereka beroperasi menggunakan PC dengan cara mengendus (*sniffing*) dan menganalisis data dalam transit di jaringan, kemudian mengekstraksi *password* terenkripsi yang ditularkan oleh pengguna selama koneksi. Jika pelaku tidak bisa mengandalkan keterlibatan dari dalam organisasi dalam mendapatkan *password* secara langsung, maka dengan bantuan perangkat elektronik mereka dapat mencegatnya dari protokol komunikasi atau mengakses file yang berisi semua *password*.
- *Trojan Horse*. Program mata-mata yang spesifik dan sangat berbahaya (*spyware*) secara diam-diam dapat merekam parameter yang digunakan untuk menghubungkannya ke sistem remote. *Trojan* adalah sebuah program kecil yang umumnya mengganti dirinya untuk kode login yang meminta pengguna untuk menangkap atau memberikan

identifikasi dan *password*, dengan keyakinan bahwa ia berada dalam lingkungan operasi normal, dimana sandi segera ditransmisikan ke server sebagai pesan anonim dari pelaku.

- Sistem Otentifikasi. Semua *password* pengguna harus disimpan pada sebuah server. Pelaku akan mengakses file yang menyimpan semua *password* user yang dienkripsi, untuk kemudian dibuka dengan utilitas yang tersedia pada jaringan.
- *Cracking Password* Terenkripsi. Jika pelaku atau *cracker* tahu *algoritma cypher*, ia bisa menguji semua permutasi yang mungkin, yang dapat merupakan kunci untuk memecahkan *password*. Serangan ini dikenal sebagai *brute force*. Alternatif lain adalah dengan menggunakan kamus untuk menemukan *password* terenkripsi, yang disebut serangan kamus. Dengan perbandingan berturut-turut, bentuk kode *password* yang terdapat dalam kamus kriminal dapat digunakan untuk menebak *password* terenkripsi yang digunakan.
- Memata-matai. Hal ini dilakukan dengan merekam parameter koneksi mereka dengan menggunakan software, *spyware* atau perangkat

multimedia, seperti kamera video dan mikrofon, guna menangkap informasi rahasia, seperti *password* untuk mengakses sistem yang dilindungi.

f) *Spam*. *Spam* adalah pengiriman e-mail secara massal yang tidak dikehendaki, dengan tujuan :

- Komersial atau publisitas.
- Memperkenalkan perangkat lunak berbahaya, seperti *malware* dan *crimeware* ke dalam sistem.
- Pada situasi terburuk, spam menyerupai serangan bom e-mail, dengan akibat mail server mengalami kelebihan beban, *mailbox user* penuh dan ketidaknyamanan dalam pengelolaan. Sebelumnya spam hanya dianggap sebagai gangguan, tapi saat ini e-mail *spam* merupakan ancaman nyata. Hal tersebut telah menjadi vektor istimewa untuk penyebaran virus, worm, trojans, spyware dan upaya *phishing*.

g) Penyalahgunaan Protokol Komunikasi. Sebuah serangan *Spoofing Transmission Control Protocol* (TCP) bergantung pada kenyataan bahwa protokol TCP menetapkan koneksi logis antara dua ujung sistem untuk mendukung pertukaran data. Pengidentifikasi

logis (nomor port) digunakan untuk membangun sebuah koneksi TCP. Sebuah serangan TCP nomor port akan melibatkan kegiatan menebak atau memprediksi nomor port berikutnya yang akan dialokasikan untuk pertukaran data dalam rangka menggunakan angka-angka bukan pengguna yang sah. Hal ini memungkinkan untuk melewati *firewall* dan mendirikan sebuah hubungan yang aman antara dua entitas, yaitu *hacker* dan target.

4) Jenis Ancaman

Menurut Michael D. McDonnell dan Terry L. Sayers, jenis ancaman siber dikelompokkan dalam :

- a) Ancaman Perangkat Keras (*hardware threat*), yaitu ancaman yang disebabkan oleh pemasangan peralatan tertentu yang berfungsi untuk melakukan kegiatan tertentu dalam suatu sistem, sehingga peralatan tsb merupakan gangguan terhadap sistem Jaringan dan Perangkat Keras lainnya, contoh : *Jamming* dan *Network Intrusion*.
- b) Ancaman Perangkat Lunak (*software threat*), yaitu ancaman yang disebabkan oleh masuknya software tertentu yang berfungsi untuk melakukan kegiatan seperti : Pencurian Informasi (*Information*

Theft), Perusakan Informasi / Sistem (Information / System Destruction), Manipulasi Informasi (*Information Corruption*) dan lain sebagainya, ke dalam suatu sistem.

- c) Ancaman Data/Informasi (*data/information threat*), adalah ancaman yang diakibatkan oleh penyebaran data/informasi tertentu yang bertujuan untuk kepentingan tertentu, seperti yang dilakukan dalam *information warfare* termasuk kegiatan propaganda.

b. Serangan Yang Mengakibatkan Terganggunya Sistem Elektronik

1) Serangan Siber

Serangan Siber (*Cyber Attack*) terjadi ketika intensitas dan skala ancaman siber meningkat dan berubah dari ancaman yang bersifat potensial menjadi faktual berupa kegiatan atau tindakan yang bertujuan untuk memasuki, menguasai, memodifikasi, mencuri atau merusak, atau menghancurkan atau melumpuhkan sistem atau aset informasi, yang dikategorikan, sebagai berikut :

- a) Perang Siber (*Cyber war*), adalah semua tindakan yang dilakukan secara sengaja dan terkoordinasi dengan tujuan mengganggu kedaulatan negara. Perang siber dapat berupa serangan terorisme (*cyber terrorism*) maupun spionase (*cyber espionage*) yang mengganggu keamanan

nasional. Adapun serangan siber memiliki karakteristik sebagai berikut :

- *Intentional* (disengaja).
- Kegiatan aktif.
- Skala besar.

b) Gangguan Siber (*Cyber Violence*), adalah serangan siber yang memiliki karakteristik sebagai berikut :

- *Unintentional* (Tidak disengaja)
- Kegiatan pasif
- Skala kecil

2) Penanggulangan Serangan Siber

Kegiatan penanggulangan serangan siber menggunakan pendekatan yang menyesuaikan diri dengan sumber dan bentuk serangan yang dihadapi. Bentuk penanggulangan serangan siber yang dilakukan dapat berupa :

- a) Pertahanan siber (*cyber defense*), adalah suatu upaya untuk menanggulangi serangan siber yang menyebabkan terjadinya gangguan terhadap penyelenggaraan negara secara normal. Pertahanan siber disiapkan sebagai suatu upaya penanggulangan serangan siber semacam ini.
- b) Penanganan secara hukum. Melakukan koordinasi dengan aparat keamanan terkait apabila telah diketahui pelaku kejahatan siber.

c) Serangan balik siber (*Cyber counter-attack*), adalah suatu tindakan serangan balik terhadap sumber serangan dengan tujuan memberikan efek jera terhadap pelaku serangan siber.

3) Sasaran Serangan Siber

Berdasarkan tujuan dan sasarannya, serangan siber ditujukan kepada :

- a) Perorangan, masyarakat umum, organisasi, komunitas tertentu, yang bersifat kejahatan siber.
- b) Obyek Vital Infrastruktur Kritis Nasional (*National Critical Infrastructure*), yaitu sistem-sistem infrastruktur fisik yang sangat penting dimana bila sistem ini tidak berfungsi atau rusak, maka dapat berdampak melemahkan pertahanan atau keamanan serta ekonomi bangsa.
- c) Kepentingan nasional, yaitu seluruh aspek yang terkait dengan tujuan nasional, lambang / simbol negara, politik negara serta kepentingan bangsa.

4) Dampak Serangan Siber

Dampak yang mungkin dialami dari sebuah serangan siber dapat berbentuk :

- a) Gangguan fungsional.
- b) Pengendalian sistem secara *remote*.
- c) Penyalahgunaan informasi.
- d) Kerusuhan, ketakutan, kekerasan, kekacauan, konflik.

- e) Serta kondisi lain yang sangat merugikan, sehingga memungkinkan dapat mengakibatkan kehancuran.²⁸

²⁸ Peraturan Menteri Pertahanan Republik Indonesia Nomor 32 Tahun 2014 Tentang Pedoman Pertahanan Siber, 6-15.

BAB III
PUTUSAN PENGADILAN NEGERI UNAAHA
NOMOR 25/PID.SUS/2019/PN UNH TENTANG
TINDAK PIDANA YANG BERAKIBAT
TERGANGGUNYA SISTEM ELEKTRONIK

A. Posisi Kasus

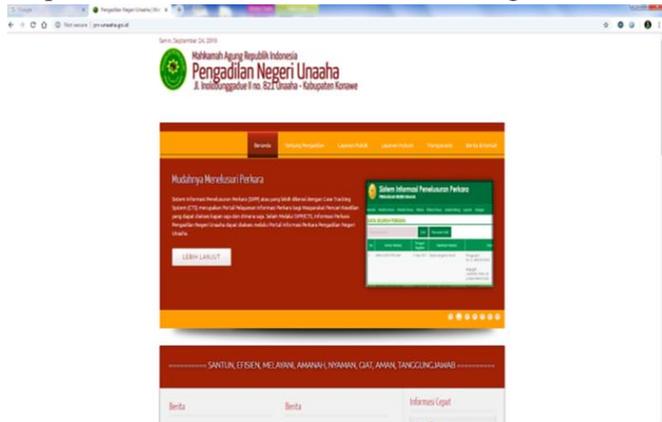
Putusan Pengadilan Negeri Unaha Nomor 25/Pid.Sus/2019/PN Unh merupakan tetapan hukum atas tindak pidana yang berakibat terganggunya system elektronik pada *website* milik Pengadilan Negeri Unaha.

Kasus ini terjadi pada hari Sabtu, tanggal 30 Juni 2018, seorang pemuda berusia 19 tahun bernama L melakukan *defacement* terhadap *website* Pengadilan Negeri Unaha, Sulawesi Tenggara. L adalah seorang pemuda yang memiliki ketertarikan dalam bidang *defacement website*.

Defacement adalah tindakan mengubah tampilan *website* tanpa izin dari pemiliknya. Bermula dari kesukaan Terdakwa L dalam melakukan *defacement website*. Pada saat itu, L sedang berada di rumahnya di Dsn Bedrek Utara RT 004/002 Desa Grogol Kecamatan Grogol Kabupaten Kediri Jawa Timur. Ia menggunakan laptop miliknya untuk mencari target *defacement*. Pada pukul 20.00 WIB, L menggunakan web browser Google.com untuk mencari situs-situs Indonesia yang menggunakan komponen Com_Fabrik.

Com_Fabrik adalah komponen yang sering digunakan untuk membuat situs hukum. L menemukan situs jdih1.pn-unaaha.go.id, situs *website* milik Pengadilan Negeri Unaha. Situs tersebut menggunakan komponen Com_Fabrik. L kemudian mencoba mengeksploitasi bug pada situs tersebut. L berhasil menemukan bug pada

halaman "files;patch". Bug tersebut memungkinkannya untuk mengupload file ke situs tersebut. L kemudian mengupload *script* berbentuk *file* html yang berfungsi sebagai tampilan *website*. Setelah berhasil mengupload *script* tersebut, L berhasil mengubah tampilan user *interface* dari *website* Pengadilan Negeri Unaaha. Tampilan awal *website* tersebut adalah sebagai berikut:



Setelah di-deface oleh L, tampilan *website* tersebut berubah menjadi sebagai berikut:



Tampilan website tersebut menampilkan gambar bayi yang sekedar memakai celana dalam dan tulisan "*Dont Touch Website*". Tampilan tersebut juga menampilkan link ke grup WhatsApp buatan L sendiri, X-Friends Cyber Team. Setelah berhasil melakukan *deface* situs Pengadilan Negeri Unaaha tersebut, L mengirimkan *screenshot* hasil *defacement* tersebut ke grup WhatsApp X-Friends Cyber Team yang beranggotakan terdakwa sendiri sebagai/1 (*admin*) dengan tujuan sebagai dokumen pribadi, akibat perbuatan *defacement* tersebut, sistem elektronik pada *website* Pengadilan Negeri Unaaha terganggu. Baik pegawai maupun masyarakat yang akan menggunakan situs *website* Pengadilan Negeri Unaaha menjadi terganggu dan tidak dapat mengaksesnya.¹

B. Substansi Putusan

Putusan pengadilan adalah titik puncak atau akhir dari seluruh rangkaian hukum acara.² Keberadaan putusan tersebut dinantikan oleh para pencari keadilan, karena dengan putusan hakim tersebut diharapkan akan menciptakan kepastian hukum dan keadilan terkait perkara yang sedang dihadapi para pencari keadilan.

Putusan hakim disatu sisi berguna bagi terdakwa untuk memperoleh kepastian hukum tentang statusnya dalam perkara pidana dan disisi yang lain putusan hakim merupakan mahkota hakim yang harus terhindar dari kecacatan dan kekeliruan untuk mencapai nilai-nilai keadilan dalam masyarakat. Putusan pengadilan

¹ Putusan Nomor 25/Pid.Sus/2019/PN Unh.

² Nikolas Simanjuntak, *Acara Pidana Indonesia dalam Sirkus Hukum*, (Bogor :Ghalia Indonesia, 2009), 223.

merupakan babak akhir dari proses hukum acara yang dinanti-nantikan oleh para pencari keadilan. Putusan hakim diharapkan mampu membawa kepastian hukum dan keadilan atas perkara yang dihadapi.

Bagi terdakwa, putusan hakim bagaikan mahkota yang menentukan statusnya dalam jeratan hukum pidana. Di satu sisi, putusan memberikan kepastian hukum, mengakhiri kegundahan dan ketidakpastian akan nasib mereka. Di sisi lain, putusan tersebut merupakan perwujudan keadilan yang diharapkan mampu membawa keseimbangan dan kedamaian bagi semua pihak yang terlibat. Oleh karena itu, putusan hakim harus terhindar dari cacat dan kekeliruan. Ketelitian dan kehati-hatian hakim dalam menimbang fakta, bukti, dan argumentasi menjadi kunci utama dalam menghasilkan putusan yang adil dan bermartabat. Putusan yang tepat dan berlandaskan hukum tidak hanya memberikan kepastian hukum bagi para pihak, tetapi juga menegakkan pilar keadilan dalam masyarakat.

Putusan pengadilan sebagaimana dimaksud dalam Pasal 1 Ayat 11 KUHAP:

“Pernyataan hakim yang diucapkan dalam sidang pengadilan terbuka, yang dapat berupa pemidanaan atau bebas atau lepas dari segala tuntutan hukum dalam hal ini serta menurut cara yang diatur dalam undang-undang ini.”³

Putusan tersebut tidak hanya yang diucapkan saja, namun juga pernyataan yang dituangkan dalam bentuk tertulis sebagai akta otentik. Semua putusan pengadilan

³ Pasal 1 butir 11 Kitab Undang-Undang Hukum Acara Pidana.

hanya sah dan memiliki kekuatan hukum jika diucapkan dalam sidang terbuka untuk umum.

Putusan pengadilan sering disebut juga putusan hakim. Menurut Lilik Mulyadi, putusan hakim merupakan putusan yang diucapkan oleh hakim karena jabatannya dalam persidangan perkara pidana yang terbuka untuk umum setelah melalui proses dan prosedural hukum acara pidana pada umumnya berisikan amar pemidanaan atau bebas atau pelepasan dari segala tuntutan hukum dibuat dalam bentuk tertulis dengan tujuan menyelesaikan perkara.⁴

Menurut Kitab Undang-Undang Hukum Acara Pidana, berdasarkan amarnya putusan pengadilan dapat dibedakan menjadi tiga sifat yaitu:

- 1) Putusan bebas (*vrijspraak*) adalah jika pengadilan berpendapat bahwa dari hasil pemeriksaan di sidang, kesalahan terdakwa atas perbuatan yang didakwakan kepadanya tidak terbukti secara sah dan meyakinkan, maka terdakwa diputus bebas (Pasal 191 ayat (1) KUHAP).
- 2) Putusan lepas dari segala tuntutan hukum (*onslog van alle rechtsvervolging*) adalah jika pengadilan berpendapat bahwa perbuatan yang didakwakan kepada terdakwa terbukti, tetapi perbuatan itu tidak merupakan suatu tindak pidana, maka terdakwa diputus lepas

⁴ Lilik Mulyadi, *Seraut Wajah Putusan Hakim Dalam Hukum Acara Pidana Indonesia: Perspektif, Teoritis, Praktik, Teknik Membuat Dan Permasalahannya*, (Bandung: Citra Aditya Bakti, 2014), 130.

dari segala tuntutan hukum (Pasal 191 ayat (2) KUHAP).

- 3) Putusan pemidanaan (*verordeling*) adalah jika pengadilan berpendapat bahwa terdakwa bersalah melakukan tindak pidana yang didakwakan kepadanya, maka pengadilan menjatuhkan pidana (Pasal 193 ayat (1) KUHAP)

Putusan hakim atau putusan pengadilan menurut Pasal 197 KUHAP memuat kepala putusan, identitas terdakwa ditulis lengkap, dakwaan, pertimbangan mengenai fakta dan keadaan serta alat pembuktian, tuntutan pidana, pasal peraturan perundang-undangan yang menjadi dasar hukum putusan dan dasar pemidanaan disertai keadaan yang memberatkan dan yang meringankan terdakwa, pernyataan kesalahan terdakwa, pernyataan terpenuhi semua unsur pidana disertai pemidanaan yang dijatuhkan, ketentuan biaya perkara dibebankan dan ketentuan barang bukti, perintah terdakwa ditahan atau tetap dalam tahanan atau dibebaskan, hari dan tanggal putusan, nama penuntut umum, nama hakim yang memutus, dan nama panitera.⁵ Berdasarkan perkara tentang terhadap terganggunya sisten elektronik menurut Putusan Pengadilan

⁵ Usman Pakaya, "Bahasa Hukum Dalam Putusan Perkara Pidana"*Negara Hukum* vol. 8, no. 1 (2017), 158.

Unaha Nomor 25/Pid.Sus/2019/PN Unh,
memuat identitas terdakwa antara lain:

Nama : L;
Tempat Lahir : Kediri;
Umur/Tanggal Lahir : 19 Tahun/9 November 1999;
Jenis Kelamin : Laki-Laki;
Kebangsaan : Indonesia;
Tempat Tinggal : Dsn Bedrek Utara RT 004/002 Desa Grogol, Kec. Grogol, Kab. Kediri, Prov. Jawa Timur;
Agama : Islam;
Pekerjaan : Belum/Tidak Bekerja;
Pendidikan : MA (Madrasah Aliyah);

Terdakwa ditahan dalam Rumah Tahanan Negara oleh Penyidik sejak tanggal 27 September 2018 sampai dengan tanggal 16 Oktober 2018. Penahanan kemudian diperpanjang oleh Penuntut Umum sejak tanggal 17 Oktober 2018 sampai dengan tanggal 25 November 2018.

Selanjutnya, perpanjangan pertama dilakukan oleh Ketua Pengadilan Negeri Unaaha sejak tanggal 26 November 2018 sampai dengan tanggal 25 Desember 2018, dan perpanjangan kedua oleh Plh. Ketua Pengadilan Negeri Unaaha sejak tanggal 26 Desember 2018 sampai dengan tanggal 24 Januari 2019.

Penuntut Umum kembali menahan terdakwa sejak tanggal 7 Januari 2019 sampai dengan tanggal 5 Februari 2019. Penahanan dilanjutkan oleh Majelis Hakim Pengadilan Negeri Unaaha sejak tanggal 30 Januari 2019

sampai dengan tanggal 28 Februari 2019. Terakhir, perpanjangan dilakukan oleh Ketua Pengadilan Negeri Unaaha sejak tanggal 1 Maret 2019 sampai dengan tanggal 29 April 2019.⁶

Penuntut Umum mengajukan tuntutan pidana terhadap Terdakwa L dengan poin-poin utama sebagai berikut:

Pertama, menyatakan bahwa Terdakwa L terbukti secara sah dan meyakinkan bersalah melakukan tindak pidana “dengan sengaja melakukan tindakan yang berakibat terganggunya sistem elektronik dan/atau tidak bekerja sebagaimana mestinya”, sebagaimana dalam dakwaan Kesatu Primair Pasal 49 Jo Pasal 33 UU No. 19 Tahun 2016 tentang Perubahan atas UU RI No. 11 Tahun 2008 tentang ITE, yang tercantum dalam Surat Dakwaan Penuntut Umum.

Kedua, menjatuhkan pidana kepada Terdakwa L dengan pidana penjara selama 2 (dua) tahun, dikurangi selama Terdakwa berada dalam masa penahanan sementara, dengan permintaan agar Terdakwa tetap ditahan.

Ketiga, barang bukti berupa 1 (satu) *bundle screenshot* tampilan *website* Pengadilan Negeri Unaaha yang telah di-*deface*; 1 (satu) *bundle screenshot* tampilan yang telah di-*deface*; 1 (satu) buah flashdisk berisi file log akses pada bulan Juni 2018 *website* Pengadilan Negeri Unaaha; 1 (satu) lembar bukti pembayaran langganan PT. TELKOM INDONESIA (Speedy) dengan No. JASTEI: 152640212851 tetap terlampir dalam berkas perkara; 1 (satu) handphone merk Lenovo type A7000-A dengan sim card Telkomsel ICCID 62100037826108540 dan memory

⁶ Putusan Nomor 25/Pid.Sus/2019/PN Unh.

micro SD-8GB; 1 (satu) handphone merk ASUS Z00ED dengan simcard Telkomsel; 1 (satu) unit laptop merk ACER type ASPIRE E1-471; dan 1 (satu) flashdisk merk Toshiba warna putih kapasitas 8 GB dirampas untuk dimusnahkan.

Keempat, membebankan kepada Terdakwa untuk membayar biaya perkara sebesar Rp 5.000,00 (lima ribu rupiah). Dalam persidangan, Terdakwa tidak didampingi oleh penasihat hukum, namun pada pokoknya Terdakwa menyesal atas perbuatannya, berjanji tidak akan mengulangi lagi, dan memohon keringanan hukuman.

a) Dakwaan Penuntut Umum

Setelah mendengar tanggapan dari Penuntut Umum terhadap permohonan Terdakwa yang intinya tetap pada tuntutan semula, Majelis Hakim mempertimbangkan bahwa Terdakwa diajukan ke persidangan dengan dakwaan sebagai berikut:

Dakwaan Primair, yaitu perbuatan Terdakwa L yang didakwa melanggar Pasal 49 Jo. Pasal 33 UU RI No.19 Tahun 2016 tentang Perubahan atas UU RI No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Dakwaan Subsidair, yaitu perbuatan Terdakwa Lanang Yoga yang didakwa melanggar Pasal 48 ayat (1) Jo. Pasal 32 ayat (1) UU RI No.19 Tahun 2016 tentang Perubahan atas UU RI No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Dakwaan Lebih Subsidair Pertama, yaitu perbuatan Terdakwa L yang didakwa melanggar Pasal 46 ayat (3) Jo. Pasal 30 ayat (3) UU RI No.19 Tahun

2016 tentang Perubahan atas UU RI No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Dakwaan Lebih Subsidair Kedua, yaitu perbuatan Terdakwa L yang didakwa melanggar Pasal 50 ayat (3) Jo. Pasal 22 huruf b UU RI No.19 Tahun 2016 tentang Perubahan atas UU RI No.36 Tahun 1999 tentang Telekomunikasi.

b) Keterangan Saksi dan Ahli

Untuk membuktikan dakwaanya, maka penuntut umum dipersidangan mengajukan alat bukti yakni keterangan saksi dan alat bukti yang digunakan oleh terdakwa. Pada perkara ini penuntut umum mengajukan alat bukti berupa keterangan dari 5 (lima) orang saksi yang dihadapkan di muka persidangan dan 3 (Tiga) orang saksi ahli yang dimana telah dipanggil secara patut tidak juga hadir di persidangan maka atas permintaan Penuntut Umum setelah Terdakwa menyatakan persetujuannya, maka keterangan Para Saksi yang ada dalam Berita Acara Pemeriksaan Penyidik dibawah sumpah lalu di bacakan oleh Penuntut Umum di persidangan. Adapun saksi-saksi tersebut masing-masing diantaranya menerangkan sebagai berikut:

a) Ramdhani Dwi Cesario, S.H., S.I.K memberikan keterangan sebagai berikut:

Saksi tidak mengenal Terdakwa dan tidak memiliki hubungan keluarga maupun pekerjaan dengannya. Saksi adalah anggota kepolisian yang bertugas di Direktorat Tindak Pidana Siber Bareskrim Polri dengan tugas melakukan penyelidikan, patroli *cyber*, dan penyidikan terkait tindak pidana di

bidang Siber atau Dunia Maya/*Cybercrime*. Pada hari Sabtu, 30 Juni 2018, sekitar pukul 20.20 WIB, di kantor Pengadilan Negeri Unaaha, terjadi laporan polisi tentang tindak pidana *deface* terhadap *website* milik Pengadilan Negeri Unaaha dengan alamat <http://pnunaaha.go.id>. *Deface* tersebut menyebabkan tampilan *website* berubah dan mengganggu aktivitas Pengadilan Negeri Unaaha dalam mengunggah informasi dan berita, sehingga masyarakat tidak dapat memperoleh informasi tentang Pengadilan Negeri Unaaha melalui *website* tersebut. Setelah dilakukan analisis log akses, diketahui bahwa pelaku *deface* menggunakan IP Address lokal. Melalui koordinasi dengan Pengadilan Negeri Unaaha dan perusahaan *hosting website*, didapatkan enam IP Address yang diduga melakukan penyerangan, salah satunya adalah IP address 180.247.202.104, yang terdaftar atas nama Sulastri di Bedrek Utara No. RT 04/02 Grogol, Kediri, Jawa Timur. Terdakwa, L, melakukan *deface* terhadap *website* Pengadilan Negeri Unaaha dengan mengubah tampilannya. Saksi melakukan *screenshot* tampilan *website* yang telah *dideface* dan mendapatkan informasi bahwa *website* tersebut dihosting oleh PT. Myindo *Cyber Media*. *Website* Pengadilan Negeri Unaaha *dideface* oleh beberapa nickname, yaitu ANSHAR CALIPHATE ARMY, X-Friends Cyber Team/R4F1_144, ngoROx, BOBOY, dan "Mr.g03nj4t404!!". Tindakan Terdakwa melakukan *deface website* Pengadilan Negeri Unaaha dapat

merusak sistem Pengadilan Negeri Unaaha, menyebabkan halaman *website* digantikan dengan halaman yang tidak terotorisasi, sehingga *website* tidak berfungsi sebagaimana mestinya. Saksi bersama rekannya kemudian melakukan penangkapan terhadap Terdakwa di rumahnya.

- b) Hari Wibowo, S.kom memberikan keterangan sebagai berikut:

Saksi adalah anggota kepolisian yang bertugas di Direktorat Tindak Pidana Siber Bareskrim Polri Unit II Subdit II, satu tim dengan Ramdhani Dwi Cesario dan Vebrian Adhi Pratama, yang bertugas melakukan penyelidikan, patroli *cyber*, dan penyidikan terkait tindak pidana di bidang Siber/Dunia Maya/*Cybercrime*. Terjadi laporan polisi tentang *deface website* Pengadilan Negeri Unaaha dengan alamat <http://pnunaaha.go.id>, yang menyebabkan Pengadilan Negeri Unaaha tidak dapat mengunggah informasi dan berita ke *website*, sehingga masyarakat tidak bisa memperoleh informasi. Setelah analisis log akses dilakukan, ditemukan enam IP Address yang diduga melakukan penyerangan, salah satunya adalah IP address 180.247.202.104 atas nama Sulastri di Bedrek Utara No. RT 04/02 Grogol, Kediri, Jawa Timur. Terdakwa melakukan perubahan tampilan *website* tersebut. Saksi melakukan *screenshot* tampilan *website* yang telah *dideface*. *Website* tersebut di-*deface* dengan nickname ANSHAR CALIPHATE ARMY, X-Friends Cyber Team/R4F1_144, ngoROx, BOBOY, dan

"Mr.g03nj4t404!". Tampilan *deface* berupa gambar bayi joget dilakukan oleh L alias Mr. L4m4, anak dari Sulastri. Saksi bersama rekannya kemudian menangkap L di rumahnya.

- c) Vebrian Adhi Pratama, S.H. memberikan keterangan sebagai berikut:

Pada hari Sabtu, 30 Juni 2018, sekitar pukul 20.20 WIB, *website* Pengadilan Negeri Unaaha mengalami gangguan saat akan mengunggah informasi dan berita. Gangguan ini menghambat pekerjaan Pengadilan Negeri Unaaha dan menyebabkan masyarakat tidak dapat memperoleh informasi tentang Pengadilan Negeri Unaaha melalui *website* tersebut.

- d) Reynold Sandu, S.T. memberikan keterangan sebagai berikut:

Pada Pengadilan Negeri Unaaha, Saksi menjabat sebagai Kepala Urusan Umum. Perusahaan *hosting website* Pengadilan Negeri Unaaha adalah PT Myindo Cyber Media dengan *domain* pn-unaaha.go.id. Pada 3 Oktober, sub domain Pengadilan Negeri Unaaha mencakup sip.pn-unaaha.go.id, tilang.pn-unaaha.go.id, dan webaru.pn-unaaha.go.id, tetapi jdih1.pn-unaaha.go.id saat ini tidak aktif. Pada bulan Juni dan Juli 2018, *website* ini mengalami *deface* oleh seorang *hacker* yang menampilkan gambar bayi berjoget, bendera Palestina dan Indonesia, serta pesan dari "Hacked by ngOROx", "Hacked by Friends Cyber Team", dan "Hacked by/R4F1-144". Tampilan awal *website* berbeda jauh dari yang di-

deface. File log menunjukkan beberapa IP address terlibat dalam serangan ini: 180.247.202.104, 180.253.162.80, 180.242.15.147, 180.247.132.32, 26.80.8.226, 36.72.101.155, dan 36.84.152.125. Serangan ini menyebabkan *website* tidak dapat diakses oleh pegawai dan masyarakat serta merusak sistem keamanan. Mahkamah Agung memberikan teguran kepada Pengadilan Negeri Unaaaha sebagai akibat dari *deface* tersebut.

- e) Timbul Wahono, S.H. memberikan keterangan sebagai berikut:

Saksi yang merupakan Panitera pengganti dan diperbantukan di bidang IT pada Pengadilan Negeri Unaaaha, menjelaskan bahwa *website* Pengadilan Negeri Unaaaha dihosting oleh PT Myindo Cyber Media dengan *domain* www.pn-unaaha.go.id. Pada tanggal 3 Oktober, sub domain aktif adalah sip.pn-unaaha.go.id, tilang.pn-unaaha.go.id, dan webaru.pn-unaaha.go.id, sementara sub domain jdih1.pn-unaaha.go.id tidak diaktifkan. *Website* ini di-*deface* oleh *hacker* pada bulan Juni dan Juli 2018. Bukti *screenshot* menunjukkan gambar bayi berjoget, bendera Palestina dan Indonesia, serta tulisan "Hacked by ngOROX", "Hacked by Friends Cyber Team", dan "Hacked by/R4F1-144". Tampilan awal *website* berbeda dengan yang di-*deface*. File log akses bulan Juni dan Juli 2018 menunjukkan beberapa IP address yang diduga terlibat dalam *deface*: 180.247.202.104, 180.253.162.80, 180.242.15.147, 180.247.132.32, 26.80.8.226, 36.72.101.155, dan 36.84.152.125.

Deface tersebut menyebabkan *website* tidak dapat diakses oleh pegawai maupun masyarakat, serta merusak sistem keamanan *website*. Akibatnya, Pengadilan Negeri Unaaha menerima teguran dari Mahkamah Agung.

Keterangan Saksi ahli sebagai berikut:

- a) Denden Imadudin Soleh, S.H., M.H. CLA menerangkan sebagai berikut:

Saksi ahli adalah Pegawai Negeri Sipil di bagian Hukum dan Kerjasama Setditjen Aplikasi Informatika Kemkominfo Republik Indonesia. Ia bekerja sebagai analis hukum dan staf di Subbagian Penelaahan dan Bantuan Hukum, dengan tugas menganalisis serta memberikan konsultasi hukum di bidang informatika, serta memberikan penjelasan mengenai Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Pada bulan Juni dan Juli 2018, terdakwa melakukan *deface website* Pengadilan Negeri Unaaha di <http://pnunaaha.go.id> pada pukul 22.22 WIB, menggunakan IP *address* lokal yang berbeda-beda. Akibat *deface* tersebut, *website* Pengadilan Negeri Unaaha menjadi tidak dapat diakses, menghambat pegawai dalam mengunggah informasi dan berita, serta menyulitkan masyarakat dalam mencari informasi di situs tersebut.

- b) Gunawan Hutagalung, S.T., M.T menerangkan sebagai berikut:

Saksi Ahli bekerja sebagai Pegawai Negeri Sipil di Direktorat Telekomunikasi Kemkominfo Republik Indonesia, menjabat sebagai Kasubdit Jasa Telekomunikasi. Ia menjelaskan bahwa Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi mengatur penyelenggaraan telekomunikasi, termasuk tindak pidana yang melibatkan perbuatan-perbuatan terlarang dalam penyelenggaraan tersebut. Tindakan terdakwa menyebabkan kerusakan pada sistem *website* dan menghambat aktivitas Pengadilan Negeri Unaaha.

Aditya Kurniawan, S.Kom., MMSI menjelaskan bahwa ia adalah analis hukum di Bagian Hukum dan Kerjasama Setditjen Aplikasi Informatika Kemkominfo Republik Indonesia, bekerja sebagai staf di Subbagian Penelaahan dan Bantuan Hukum. Tugasnya mencakup menganalisis dan memberikan konsultasi hukum di bidang informatika serta memberikan penjelasan terkait Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Saksi diperlihatkan tampilan user interface dari *website* Pengadilan Negeri Unaaha yang telah di-*deface*. Ia mengamati bahwa *deface* dilakukan dengan menggunakan IP *address* lokal pada waktu yang berbeda-beda. Log akses menunjukkan bahwa IP *address* 180.247.202.104 digunakan untuk mencoba mengirimkan objek menggunakan metode POST, diduga mengeksplorasi fitur file

upload untuk mengganti atau menambahkan nama domain.

Saksi menjelaskan bahwa kelemahan *website* Pengadilan Negeri Unaaha terletak pada panel yang berhasil dibobol oleh *defacer*. Ia menegaskan bahwa *deface* benar-benar merusak halaman *website* asli dan menggantinya dengan halaman baru, biasanya pada halaman indeks. *Defacer* mengganti halaman tersebut dengan gambar yang disukai. Saksi juga mengungkapkan bahwa terdakwa menggunakan *script* bernama bash untuk melakukan *deface website* dengan domain .id, yang bisa diunduh di <https://github.com/soracybteam/the-fake>.

c) Keterangan Terdakwa

Dalam persidangan, Terdakwa L memberikan keterangan bahwa kejadian tersebut terjadi pada tanggal 30 Juni 2018 sekitar pukul 20.00 WIB di Kantor Pengadilan Negeri Unaaha. Pada tanggal tersebut, sekitar pukul 20.00 WIB, terdakwa mencari *bug website* melalui web browser google.com dengan secara khusus menargetkan situs Indonesia. Terdakwa memasukkan inurl:/com_fabrik site:go.id dan web browser Google mencari bug secara acak dari situs Indonesia yang menjadi target terdakwa untuk dihack. Terdakwa menemukan bug pada situs pn-unaaha.go.id dan mencoba mengeksploitasi bug tersebut menggunakan com_fabrik, berhasil menemukan tulisan files;patch. Setelah itu, terdakwa mengupload script berbentuk file HTML yang berfungsi sebagai tampilan *website* dan memungkinkan penambahan file pada

website tersebut. Setelah berhasil mengupload script, terdakwa mencoba membuka situs tersebut dan berhasil.

Terdakwa memiliki grup WA bernama *X-Friends Cyber Team* yang digunakan untuk menyimpan file *deface website* yang sudah terdakwa *deface*. Terdakwa mengetahui *website* Pengadilan Negeri Unaaha sebagai target *deface* dari pencarian `inurl:/com_fabrik site:go.id`. Tampilan *website* Pengadilan Negeri Unaaha yang menampilkan gambar bayi berjoget merupakan hasil perbuatan terdakwa. Terdakwa melakukan *deface* terhadap *website* Pengadilan Negeri Unaaha dengan alamat `http://pn-unaaha.go.id` pada tanggal 30 Juni 2018 sekitar pukul 20.20 WIB, menggunakan IP address 180.247.202.104 dan koneksi internet Speedy yang terdaftar atas nama ibunya, Sulastri, beralamat di Bedrek Utara RT.04/02, Grogol, Kediri, menggunakan laptop miliknya.

Ketika terdakwa melakukan serangkaian perbuatan *deface* terhadap situs Pengadilan Negeri Unaaha, tidak ada seorang pun yang mengetahuinya secara langsung. Terdakwa melakukan tindakan ini dengan motif untuk menguji keamanan *website* tersebut. Penuntut Umum kemudian mengajukan sejumlah barang bukti untuk memperkuat dakwaannya:

Terdapat satu bundle *screenshot* tampilan *website* Pengadilan Negeri Unaaha yang telah di-*deface* dan satu bundle *screenshot* tampilan yang telah di-*deface*. Selain itu, terdapat satu buah flashdisk berisi *file log* akses pada bulan Juni 2018 untuk *website* Pengadilan Negeri Unaaha, satu lembar bukti pembayaran

langganan PT. TELKOM INDONESIA (Speedy) dengan No. JASTEI: 152640212851, satu handphone merk Lenovo tipe A7000-A dengan sim card Telkomsel ICCID 62100037826108540 dan memori micro SD 8GB, satu handphone merk ASUS Z00ED dengan simcard Telkomsel, satu unit laptop merk ACER tipe ASPIRE E1-471, dan satu flashdisk merk Toshiba warna putih dengan kapasitas 8GB.

Barang bukti yang disita secara sah menurut hukum telah diperlihatkan kepada para saksi dan terdakwa. Para saksi dan terdakwa telah mengkonfirmasi kebenaran barang bukti tersebut. Dengan demikian, barang bukti tersebut dapat digunakan untuk memperkuat pembuktian dalam perkara ini.

C. Pertimbangan Hakim

Menimbang, bahwa selanjutnya Majelis Hakim akan mempertimbangkan apakah berdasarkan fakta-fakta hukum tersebut di atas, Terdakwa dapat dinyatakan telah melakukan tindak pidana yang didakwakan kepadanya; Menimbang, bahwa Terdakwa telah didakwa oleh Penuntut Umum dengan dakwaan yang berbentuk alternatif, sehingga Majelis Hakim dengan memperhatikan fakta-fakta hukum tersebut di atas memilih langsung dakwaan alternatif Kesatu Primair sebagaimana diatur dalam Pasal 49 Jo. Pasal 33 UU RI No 19 Tahun 2019 tentang Perubahan atas UU RI No 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang unsur-unsurnya adalah sebagai berikut:

- 1) Setiap orang;

- 2) Dengan sengaja dan tanpa hak atau melawan hukum melakukan tindakan apapun yang berakibat terganggunya sistem elektronik dan/atau mengakibatkan sistem elektronik menjadi tidak bekerja sebagaimana mestinya;

Menimbang, bahwa terhadap unsur-unsur tersebut Majelis Hakim mempertimbangkan sebagai berikut:

1) Unsur Setiap orang;

Menimbang, bahwa unsur “Setiap orang” dalam tindak pidana menunjuk kepada Subyek Hukum yaitu manusia pribadi (*Natuurlijke Persoon*) dan badan hukum (*Rechts persoon*) selaku pendukung hak dan kewajiban; Menimbang, bahwa unsur “Setiap orang” adalah untuk mengetahui siapa atau siapa saja orangnya yang didakwa atau akan dipertanggungjawabkan karena perbuatannya yang telah dilakukan sebagaimana dirumuskan di dalam surat dakwaan; Menimbang, bahwa di dalam persidangan, Penuntut Umum telah menghadapkan L yang diajukan sebagai Terdakwa setelah identitasnya diperiksa ternyata telah sesuai dengan yang tercantum dalam surat dakwaan dan Terdakwa mengakui bahwa dirinyalah orang yang didakwa sehingga tidak ditemukan terjadinya salah orang, sedangkan mengenai perbuatan Terdakwa sebagaimana dalam dakwaan akan dibuktikan perbuatannya dalam unsur selanjutnya, sehingga dengan demikian unsur “Setiap orang” telah terpenuhi;

- 2) **Unsur Dengan sengaja dan tanpa hak atau melawan hukum melakukan tindakan apapun yang berakibat terganggunya sistem elektronik dan/atau mengakibatkan sistem elektronik menjadi tidak bekerja sebagaimana mestinya;** Menimbang, bahwa berdasarkan fakta-fakta yang terjadi dipersidangan bahwa kejadian pada hari Sabtu, tanggal 30 Juni 2018 sekira pukul 20.20 WIB tepatnya di kantor Pengadilan Negeri Unaaha beralamat di Jl. Inolobungadue II No. 821 Unaaha Kabupaten Konawe Provinsi Sulawesi Tenggara; Menimbang, bahwa unsur tersebut yaitu merupakan suatu kesatuan yang dalam tataran penerapan hukum harus dapat dibuktikan oleh penegak hukum;

Menurut Prof. Satochid Kartanegara, yang dimaksud dengan *opzet willens en weten* (dikehendaki dan diketahui) adalah “Seseorang yang melakukan suatu perbuatan dengan sengaja harus menghendaki (*willen*) perbuatan itu serta harus menginsafi atau mengerti (*weten*) akan akibat dari perbuatan itu”. Bahwa “Kehendak” dapat ditujukan terhadap perbuatan yang dilarang dan akibat yang dilarang;⁷

Pengertian “kesengajaan” dalam hukum pidana dikenal 2 (dua) teori, yaitu teori kehendak (*Wilstheorie*) dan teori membayangkan (*Voorstellingstheorie*). Teori kehendak (*Wilstheorie*) dikemukakan oleh Von Hippel dalam bukunya *Die Grenze Vorsatz und*

⁷ Putusan Nomor 25/Pid.Sus/2019/PN Unh.

Fahrlässigkeit tahun 1903, yang menyatakan kesengajaan adalah kehendak membuat suatu tindakan dan kehendak menimbulkan suatu akibat dari tindakan itu. Akibat dikehendaki apabila akibat itu yang menjadi maksud dari tindakan tersebut dan teori membayangkan (*Vorstellungstheorie*) dikemukakan oleh Frank dalam bukunya *Festschrift Gieszen* tahun 1907 yang menyatakan bahwa manusia tidak mungkin dapat menghendaki suatu akibat dan manusia hanya dapat mengingini, mengharapkan dan membayangkan (*voorstellen*) kemungkinan adanya suatu akibat;⁸

Secara umum, para ahli hukum pidana menyebutkan adanya 3 (tiga) macam bentuk kesengajaan (*opzet*), yaitu:

- 1) Kesengajaan sebagai maksud (*opzet als oogmerk*), yaitu sengaja sebagai maksud menurut MvT adalah dikehendaki dan dimengerti;
- 2) Kesengajaan dengan keinsafan pasti (*opzet als zekerheidsbewustzijn*) yaitu Kesengajaan dengan keinsafan pasti yaitu si pelaku menyadari bahwa dengan melakukan perbuatan itu, pasti akan timbul perbuatan lain;
- 3) Kesengajaan dengan keinsafan kemungkinan (*dolus eventualis*) yaitu Kesengajaan dengan keinsafan kemungkinan (*dolus eventualis*) disebut juga “kesengajaan dengan kesadaran

⁸ Putusan Nomor 25/Pid.Sus/2019/PN Unh.

kemungkinan”, bahwa seseorang melakukan perbuatan dengan tujuan untuk menimbulkan suatu akibat tertentu;

Berdasarkan uraian sebelumnya, terbukti bahwa Terdakwa telah melakukan tindakan dengan sengaja dan tanpa hak atau melawan hukum yang mengakibatkan terganggunya sistem elektronik dan/atau mengakibatkan sistem elektronik menjadi tidak bekerja sebagaimana mestinya. Hal ini dibuktikan dengan terpenuhinya seluruh unsur dalam Pasal 49 Jo. Pasal 33 UU RI No.19 Tahun 2016 Tentang Perubahan Atas UU RI No.11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.

Oleh karena itu, berdasarkan bukti-bukti dan uraian di atas, dapat disimpulkan bahwa Terdakwa terbukti secara sah dan meyakinkan melakukan tindak pidana sebagaimana didakwakan dalam dakwaan Kesatu Primair.

Dalam pemeriksaan perkara di muka persidangan, Majelis Hakim tidak menemukan adanya faktor-faktor yang dapat menghapuskan pertanggungjawaban pidana Terdakwa. Baik alasan pembenar maupun alasan pemaaf, tidak terdapat satu pun yang dapat diterapkan dalam kasus ini. Oleh karena itu, Terdakwa harus mempertanggungjawabkan perbuatannya secara hukum.

Menimbang bahwa untuk menjatuhkan pidana terhadap Terdakwa maka perlu dipertimbangkan

terlebih dahulu keadaan yang memberatkan dan yang meringankan Terdakwa;

Keadaan yang memberatkan:

- Perbuatan terdakwa mengakibatkan situs/*website* Pengadilan Negeri Unaha tidak dapat diakses oleh pegawai maupun masyarakat;

Keadaan yang meringankan:

- Terdakwa mengakui terus terang perbuatannya sehingga memperlancar proses persidangan;
- Terdakwa belum pernah dihukum;

D. Amar Putusan

MENGADILI

1. Menyatakan Terdakwa L tersebut di atas, terbukti secara sah dan meyakinkan bersalah melakukan tindak pidana dengan sengaja dan tanpa hak atau melawan hukum melakukan tindakan yang berakibat terganggunya system elektronik dan mengakibatkan system elektronik menjadi tidak bekerja sebagaimana mestinya;
2. Menjatuhkan pidana kepada Terdakwa L oleh karena itu dengan pidana penjara selama 1 (satu) tahun dan 4 (empat) bulan;
3. Menetapkan masa penahanan yang telah dijalani Terdakwa dikurangkan seluruhnya dari pidana yang dijatuhkan,
4. Menetapkan Terdakwa tetap ditahan
5. Menetapkan barang bukti berupa:

- 1 (satu) *bundle screenshot* tampilan *website* Pengadilan Negeri Unaha yang telah di *deface*;
 - 1 (satu) *bundle screenshot* tampilan yang telah di *deface*;
 - 1 (satu) lembar bukti pembayaran langganan PT. TELKOM INDONESIA (Speedy) dengan No. JASTEI: 152640212851;
Tetap terlampir dalam berkas perkara;
 - 1 buah flashdisk berisi file log akses pada bulan Juni 2018 Pengadilan Negeri Unaha
 - 1 (satu) Flashdisk merk Toshiba warna putih kapasitas 8 GB;
Dirampas untuk dimusnahkan;
 - 1 (satu) handphone merk Lenovo type A7000-A dengan sim card Telkomsel ICCID 62100037826108540 dan Memorymicro SD-8GB;
 - 1 (satu) handphone merk ASUS Z00ED dengan simcard telkomsel;
 - 1 (satu) unit laptop merk ACER type ASPIRE E1-471;
 - Dirampas untuk Negara;
6. Membebaskan kepada terdakwa membayar biaya perkara sejumlah Rp 5.000,00 (Lima ribu rupiah).

BAB IV
ANALISIS PUTUSAN PENGADILAN NEGERI
UNAAHA (NOMOR 25/PID.SUS/2019/PN UNH)
TERHADAP TINDAK PIDANA YANG
MENGAKIBATKAN TERGANGGUNYA SISTEM
ELEKTRONIK

A. Pertimbangan Hukum Hakim Terhadap Tindak Pidana Yang Berakibat Terganggunya Sistem Elektronik Pada Putusan Pengadilan Negeri Unaaaha Nomor 25/Pid.Sus/2019/PN UNH

Pertimbangan hukum hakim sering dijuluki sebagai “Tangan Kanan Tuhan”, dimana hakim merupakan orang yang dipercayanya menentukan atau memutuskan benar atau salah dari perbuatan yang dilakukan oleh manusia itu sendiri. Keputusan yang dihasilkan oleh seorang hakim memegang peranan sangat penting sebagai titik kulminasi dari proses pengadilan suatu perkara yang sedang diselidiki dan dipertimbangkan oleh para hakim di Indonesia.

Pertimbangan hakim sendiri merupakan salah satu aspek terpenting dalam menentukan terwujudnya nilai dari suatu putusan hakim yang mengandung keadilan (*ex aequo et bono*) dan mengandung kepastian hukum. Selain itu, pertimbangan hakim juga mengandung manfaat bagi para pihak yang bersangkutan sehingga pertimbangan hakim ini harus disikapi dengan teliti, baik, dan cermat. Apabila pertimbangan hakim tidak teliti, baik, dan cermat, maka putusan hakim yang berasal dari pertimbangan hakim tersebut akan dibatalkan oleh Pengadilan Tinggi/Mahkamah Agung.¹ Pertimbangan hakim

¹ Mukti Arto, *Praktek Perkara Perdata pada Pengadilan Agama*, cet V (Yogyakarta, Pustaka Pelajar, 2004), 140.

atau *ratio decidendi* adalah argument atau alasan yang dipakai oleh hakim sebagai pertimbangan hukum yang menjadi dasar sebelum kasus.

Menurut Undang-Undang No 48 tahun 2009 tentang Kekuasaan Kehakiman kewenangan hakim dalam memutuskan suatu perkara terdapat tiga aspek yaitu:

- a. Menerima, laporan yang telah diajukan kepada hakim, mencari keterangan dan barang bukti.
- b. Memeriksa, melihat dengan teliti berkas perkara terdakwa
- c. Memutuskan, hukuman suatu perkara yang sedang diperiksa dan diadili hakim tersebut. Ketika dalam melakukan kewenangan itu terutama dalam mengadili suatu putusan hakim merupakan mahkota dan puncak dari suatu perkara yang sedang diperiksa dan diadili hakim tersebut.²

Oleh karena itu, tentu saja hakim dalam menjatuhkan suatu putusan harus memperhatikan segala aspek yang ada didalamnya, yaitu surat dakwaan, fakta-fakta hakim dalam persidangan, keadaan masyarakat dalam persidangan. Dengan alasan-alasan atau pertimbangan sebagaimana putusan pengadilan merupakan tanggung jawab hakim dalam melaksanakan tugasnya, untuk memeriksa, mengadili dan memutuskan perkara.³ Hakim dituntut untuk mempunyai keyakinan dalam setiap penjatuhan putusan yang akan dilakukan sehingga dapat menciptakan hukum yang berdasarkan keadilan yang tidak bertentangan dengan peraturan perundang-undangan yang berlaku. Hakim harus memerhatikan keadilan berdasarkan dari:

² Rimdan, "*kekuasaan kehakiman*", (Jakarta: Prenada Media Group, 2012), 36.

³ Bambang Waluyo, "*Pidana dan Pemidanaan*", (Jakarta: Sinar Grafika, 2008), 80.

- 1) Sisi pelaku kejahatan;
- 2) Sisi korban (dampak bagi korban);
- 3) Sisi kepentingan masyarakat pada umumnya.

Hakim, sebagai representasi lembaga peradilan, memiliki peran sentral dalam menegakkan hukum dan keadilan. Kemampuan intelektual yang mumpuni, diiringi dengan moral dan integritas yang tinggi, merupakan fondasi utama bagi hakim dalam menghasilkan putusan yang adil dan bermanfaat bagi masyarakat.

Berdasarkan Undang-Undang Tentang Kekuasaan Kehakiman Pasal 53, yang berbunyi:

- 1) Dalam memeriksa dan memutus perkara, hakim bertanggung jawab atas penetapan dan putusan yang dibuatnya.
- 2) Penetapan dan putusan sebagaimana dimaksud pada ayat (1) harus memuat pertimbangan hukum hakim yang didasarkan pada alasan dan dasar hukum yang tepat dan benar.⁴

Dalam menjalankan tugasnya memutus perkara, hakim memiliki landasan hukum yang kuat. Putusan hakim harus didasarkan pada pertimbangan yang matang dan dapat diterima oleh semua pihak. Pertimbangan ini tidak boleh menyimpang dari kaidah-kaidah hukum yang berlaku. Hal ini dikenal sebagai pertimbangan hukum atau *legal reasoning*.

Pertimbangan hukum diartikan suatu tahapan dimana majelis hakim mempertimbangkan fakta yang terungkap selama persidangan berlangsung, mulai dari dakwaan, tuntutan, eksepsi dari terdakwa yang dihubungkan dengan

⁴ Undang-Undang Republik Indonesia Nomor 48 Tahun 2009 Tentang Kekuasaan Kehakiman.

alat bukti yang memenuhi syarat formil dan syarat materil, yang disampaikan dalam pembuktian, pledoi. Dalam pertimbangan hukum dicantumkan pula pasal-pasal dari peraturan hukum yang dijadikan dasar dalam putusan tersebut.⁵ Hakim dalam mengambil suatu keputusan dalam sidang pengadilan dapat mempertimbangkan beberapa aspek:⁶

- a) Kesalahan pelaku tindak pidana;
- b) Motif dan tujuan dilakukannya suatu tindak pidana;
- c) Cara melakukan tindak pidana;
- d) Sikap batin pelaku tindak pidana;
- e) Riwayat hidup dan sosial ekonomi;
- f) Sikap dan tindakan pelaku sesudah melakukan tindak pidana
- g) Pengaruh pidana terhadap masa depan pelaku;
- h) Pandangan masyarakat terhadap tindak pidana yang dilakukan oleh pelaku

Dalam kasus tindak pidana yang berakibat terganggunya sistem elektronik di Unaaha dengan putusan perkara Nomor 25/Pid.Sus/2019/PN Unh menyatakan pertimbangan hakim dalam memutus adalah sebagai berikut:

Menimbang, bahwa Terdakwa diajukan ke persidangan oleh Penuntut Umum didakwa berdasarkan surat dakwaan yang poinnya kurang lebih sebagai berikut:

⁵ Damang, Definisi Pertimbangan Hukum, *website* http://www.damang.web.id/2011/12/defenisi-pertimbangan-hukum_17.html. Diakses 20 April 2024.

⁶ Barda Nawawi Arief, *Masalah Penegakan Hukum dan Kebijakan Penanggulangan Kejahatan* (Bandung:PT Citra Aditya Bakti, 2001), 23.

Primair: Perbuatan Terdakwa L sebagaimana diatur dan diancam dalam Pasal 49 Jo. Pasal 33 UU RI No.19 Tahun 2016 Tentang Perubahan Atas UU RI No.11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik;

Subsidiar: Perbuatan Terdakwa Lanang Yoga sebagaimana diatur dan diancam dalam Pasal 48 ayat (1) Jo. Pasal 32 ayat (1) UU RI No.19 Tahun 2016 Tentang Perubahan Atas UU RI No.11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik;

Lebih Subsidiar: Perbuatan Terdakwa L sebagaimana diatur dan diancam dalam Pasal 46 ayat (3) Jo. Pasal 30 ayat (3) UU RI No.19 Tahun 2016 Tentang Perubahan Atas UU RI No.11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik atau Perbuatan Terdakwa L sebagaimana diatur dan diancam dalam Pasal 50 ayat (3) Jo. Pasal 22 huruf b UU RI No.19 Tahun 2016 Tentang Perubahan Atas UU RI No.36 Tahun 1999 Tentang Telekomunikasi;

Menimbang, bahwa Terdakwa telah didakwa oleh Penuntut Umum dengan dakwaan yang berbentuk alternatif, sehingga Majelis Hakim dengan memperhatikan fakta-fakta hukum tersebut di atas memilih langsung dakwaan alternatif Kesatu Primair sebagaimana diatur dalam Pasal 49 Jo. Pasal 33 UU RI Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-undang RI Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang Unsur unsurnya sebagai berikut:

1. Setiap Orang

2. Sengaja dan tanpa hak atau melawan hukum melakukan tindakan apapun yang berakibat terganggunya system elektronik dan/atau mengakibatkan system elektronik menjadi tidak bekerja sebagaimana mestinya.

Terhadap unsur-unsur tersebut Majelis hakim mempertimbangkan sebagai berikut:

1. Unsur Setiap Orang

Menimbang, bahwa unsur “Setiap orang” dalam tindak pidana menunjuk kepada Subyek Hukum yaitu manusia pribadi (*Natuurlijke Persoon*) dan badan hukum (*Rechts persoon*) selaku pendukung hak dan kewajiban;

Menimbang, bahwa unsur “Setiap orang” adalah untuk mengetahui siapa atau siapa saja orangnya yang didakwa atau akan dipertanggungjawabkan karena perbuatannya yang telah dilakukan sebagaimana dirumuskan di dalam surat dakwaan; Menimbang, bahwa di dalam persidangan, Penuntut Umum telah menghadapkan L yang diajukan sebagai Terdakwa setelah identitasnya diperiksa ternyata telah sesuai dengan yang tercantum dalam surat dakwaan dan Terdakwa mengakui bahwa dirinyalah orang yang didakwa sehingga tidak ditemukan terjadinya salah orang, sedangkan mengenai perbuatan Terdakwa sebagaimana dalam dakwaan akan dibuktikan perbuatannya dalam unsur selanjutnya, sehingga dengan demikian unsur “Setiap orang” telah terpenuhi;

2. Unsur Dengan sengaja dan tanpa hak atau melawan hukum melakukan tindakan apapun yang berakibat terganggunya system elektronik dan/atau mengakibatkan system elektronik menjadi tidak bekerja sebagaimana mestinya;

Menimbang, bahwa berdasarkan fakta-fakta yang terjadi dipersidangan bahwa kejadian pada hari Sabtu, tanggal 30 Juni 2018 sekira pukul 20.20 WIB tepatnya di kantor Pengadilan Negeri Unaaha beralamat di Jl. Inolobunggadue II No. 821 Unaaha Kabupaten Konawe Provinsi Sulawesi Tenggara;

Menimbang, bahwa unsur tersebut yaitu merupakan suatu kesatuan yang dalam tataran penerapan hukum harus dapat dibuktikan oleh penegak hukum; Menimbang, bahwa menurut Prof. Satochid Kartanegara, yang dimaksud dengan *opzet willens en weten* (dikehendaki dan diketahui) adalah “Seseorang yang melakukan suatu perbuatan dengan sengaja harus menghendaki (*willen*) perbuatan itu serta harus menginsafi atau mengerti (*weten*) akan akibat dari perbuatan itu”. Bahwa “Kehendak” dapat ditujukan terhadap perbuatan yang dilarang dan akibat yang dilarang;

Menimbang, bahwa pengertian “kesengajaan” dalam hukum pidana dikenal 2 (dua) teori, yaitu teori kehendak (*Wilstheorie*) dan teori membayangkan (*Voorstellingstheorie*). Teori kehendak (*Wilstheorie*), yang menyatakan kesengajaan adalah kehendak membuat suatu tindakan dan kehendak menimbulkan suatu akibat dari tindakan itu. Akibat dikehendaki apabila akibat

itu yang menjadi maksud dari tindakan tersebut dan teori membayangkan (*Voorstellingstheorie*), yang menyatakan bahwa manusia tidak mungkin dapat menghendaki suatu akibat dan manusia hanya dapat mengingini, mengharapkan dan membayangkan (*voorstellen*) kemungkinan adanya suatu akibat;

Menimbang, bahwa secara umum, para ahli hukum pidana menyebutkan adanya 3 (tiga) macam bentuk kesengajaan (*opzet*), yaitu;

1. Kesengajaan sebagai maksud (*opzet als oogmerk*), yaitu sengaja sebagai maksud menurut MvT adalah dikehendaki dan dimengerti;
2. Kesengajaan dengan keinsafan pasti (*opzet als zekerheidsbewustzijn*) yaitu Kesengajaan dengan keinsafan pasti yaitu si pelaku menyadari bahwa dengan melakukan perbuatan itu, pasti akan timbul perbuatan lain;
3. Kesengajaan dengan keinsafan kemungkinan (*dolus eventualis*) yaitu Kesengajaan dengan keinsafan kemungkinan (*dolus eventualis*) disebut juga “kesengajaan dengan kesadaran kemungkinan”, bahwa seseorang melakukan perbuatan dengan tujuan untuk menimbulkan suatu akibat tertentu;

Selanjutnya untuk menjatuhkan pidana terhadap Terdakwa maka perlu dipertimbangkan terlebih dahulu keadaan yang memberatkan dan yang meringankan Terdakwa;

Keadaan yang memberatkan:

- Perbuatan Terdakwa mengakibatkan situs/*website* Pengadilan Negeri Unaaha tidak dapat di akses oleh pegawai maupun masyarakat;

Keadaan yang meringankan:

- Terdakwa mengakui terus terang perbuatannya sehingga memperlancar proses persidangan;
- Terdakwa belum pernah dihukum;

Berdasarkan pertimbangan di atas, Majelis Hakim berkesimpulan bahwa perbuatan Terdakwa telah memenuhi unsur-unsur Pasal 49 Jo. Pasal 33 UU RI No.19 Tahun 2016 tentang Perubahan Atas UU RI No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, yaitu dengan sengaja dan tanpa hak atau melawan hukum melakukan tindakan apa pun yang berakibat terganggunya sistem elektronik dan/atau mengakibatkan sistem elektronik menjadi tidak bekerja sebagaimana mestinya. Oleh karena itu, Terdakwa dinyatakan sah dan terbukti secara sah dan meyakinkan melakukan tindak pidana sebagaimana didakwakan dalam dakwaan Kesatu Primair.

Dalam persidangan, Majelis Hakim tidak menemukan hal-hal yang dapat menghapuskan pertanggungjawaban pidana Terdakwa, baik sebagai alasan pembenar maupun alasan pemaaf. Oleh karena itu, Terdakwa harus mempertanggungjawabkan perbuatannya. Terdakwa terbukti secara sah dan meyakinkan melakukan tindak pidana sebagaimana didakwakan dalam dakwaan Kesatu Primair dan tidak ditemukan alasan pembenar maupun alasan pemaaf untuk membebaskan Terdakwa dari tanggung jawab pidana

Berdasarkan analisis yang telah dilakukan, penulis sependapat bahwa apa yang diputuskan dan dijatuhkan kepada Terdakwa L oleh Majelis Hakim sudah benar dan sesuai dengan ketentuan yang berlaku. Penulis membenarkan tindakan Majelis Hakim dalam memutus perkara tersebut, salah satunya didasarkan pada

pertimbangan yuridis sesuai dengan ketentuan peraturan perundang-undangan yang berlaku. Pertimbangan yuridis merujuk pada proses penilaian dan analisis hakim yang didasarkan pada fakta-fakta terhadap berbagai aspek yang berkaitan dengan hukum dalam konteks pengambilan keputusan, terutama dalam ranah peradilan. Dalam pertimbangannya, penulis sependapat dengan apa yang telah terbukti di persidangan, meliputi: dakwaan Jaksa Penuntut Umum, keterangan Terdakwa, keterangan saksi-saksi, barang bukti persidangan, serta unsur-unsur tindak pidana yang terpenuhi. Dengan tegas, Terdakwa sendiri membenarkan perbuatannya dalam melakukan tindak pidana yang berakibat terganggunya sistem elektronik pada *website* Pengadilan Negeri Unaaha, Sulawesi Tenggara. Hal ini menjadi pertimbangan Majelis Hakim untuk memutuskan bahwa apa yang dilakukan Terdakwa benar melanggar ketentuan yang berlaku pada hukum pidana.

Selain itu, penulis menilai Majelis Hakim telah memberikan pertimbangan yang tegas dan adil dalam memutuskan hal-hal yang memberatkan dan meringankan hukuman bagi Terdakwa, khususnya dalam perkara tersebut. Adapun keadaan yang memberatkan adalah perbuatan Terdakwa mengakibatkan situs/*website* Pengadilan Negeri Unaaha tidak dapat diakses oleh pegawai maupun masyarakat. Sementara keadaan yang meringankan meliputi Terdakwa mengakui terus terang perbuatannya sehingga memperlancar proses persidangan, serta Terdakwa belum pernah dihukum sebelumnya. Oleh karena itu, Terdakwa dinyatakan sah dan terbukti secara sah dan meyakinkan melakukan tindak pidana sebagaimana didakwakan dalam dakwaan Kesatu Primair. Dalam persidangan, Majelis

Hakim tidak menemukan hal-hal yang dapat menghapuskan pertanggungjawaban pidana Terdakwa, baik sebagai alasan pembeda maupun alasan pemaaf. Oleh karena itu, Terdakwa harus mempertanggungjawabkan perbuatannya. Terdakwa terbukti secara sah dan meyakinkan melakukan tindak pidana sebagaimana didakwakan dalam dakwaan Kesatu Primair dan tidak ditemukan alasan pembeda maupun alasan pemaaf untuk membebaskan Terdakwa dari tanggung jawab pidana.

B. Analisis Yuridis Terhadap Tindak Pidana yang Berakibat Terganggunya Sistem Elektronik Dalam Putusan Pengadilan Negeri Unaha Nomor 25/Pid.Sus/2019/PN UNH

Pengertian tindak pidana dalam hukum pidana diartikan sebagai "*strafbaar feit*" yang diartikan sebagai "tindak pidana" atau "perbuatan pidana." Tindak pidana merupakan perbuatan yang melanggar undang-undang dan dikenai sanksi pidana. suatu perbuatan dapat dikategorikan sebagai tindak pidana apabila perbuatan tersebut diatur dalam undang-undang.

Hal tersebut sesuai berdasarkan Menurut Moeljatno yang menjelaskan bahwa tindak pidana adalah perbuatan manusia yang melanggar hukum, dirumuskan dalam undang-undang, dapat dipertanggung jawabkan, dan dilakukan dengan unsur kesalahan. Istilah lain yang digunakan untuk tindak pidana adalah "*delict*" yang berasal dari bahasa Latin "*delictum*" yang berarti kesalahan. Dalam bahasa Belanda, "*feit*" berarti "sebagian dari suatu kenyataan" dan "*strafbaar*" berarti "dapat dihukum," sehingga "*strafbaar feit*" secara harfiah dapat

diartikan "sebagian dari suatu kenyataan yang dapat dihukum." Penggunaan istilah "tindak pidana" dipilih untuk menjaga konsistensi dalam peraturan perundang-undangan dan literatur hukum pidana.⁷

Tindak pidana dalam KUHP dibagi menjadi tindak pidana kejahatan (*misdrijven*) dan pelanggaran (*overtredingen*). dalam hukum pidana, terdapat dua pandangan utama tentang pengertian dan unsur-unsur tindak pidana, yaitu pandangan monistis dan pandangan dualistis. Pandangan monistis yaitu bahwa tindak pidana adalah suatu perbuatan yang melanggar hukum dan memiliki unsur-unsur yang tidak dapat dipisahkan. Artinya, tindak pidana dianggap sebagai suatu kesatuan yang utuh. Sementara pandangan dualistis yaitu pandangan yang memisahkan antara perbuatan pidana dan pertanggungjawaban pidana. Menurut pandangan ini, suatu perbuatan baru dapat disebut sebagai tindak pidana jika memenuhi dua hal, yaitu perbuatan tersebut melanggar hukum (perbuatan pidana) dan pelakunya dapat dipertanggungjawabkan secara pidana (pertanggungjawaban pidana).⁸

Dalam tindak pidana terdapat juga unsur-unsur tindak pidana yang dibagi menjadi dua jenis yaitu unsur subjektif dan unsur objektif. Unsur subjektif adalah unsur-unsur

⁷ Yolanda Sari KS, dkk, "Analisis Yuridis Terhadap Tindak Pidana Manipulasi Informasi Pengguna E-Commerce Menurut Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik: Studi Putusan No. 542/Pid.Sus/2019/PN.Mlg". Locus: *Jurnal Konsep Ilmu Hukum*, vol. 2, no. 2, Juni 2022, 59.

⁸ Valentina Pinky Kristinawati, and Edi Pranoto. "Tinjauan Yuridis Terhadap Tindak Pidana Bullying Di Sekolah", *Concept: Journal of Social Humanities and Education*, vol. 2, no. 1, Mar. 2023, 60.

yang berkaitan dengan keadaan atau sikap batin pelaku, seperti Kesengajaan (*dolus*) yaitu pelaku melakukan perbuatan dengan sengaja, Niat (*mens rea*) yaitu Pelaku memiliki niat atau kehendak untuk melakukan perbuatan pidana tersebut. Sementara itu unsur objektif adalah unsur-unsur yang berkaitan dengan keadaan di luar pelaku, seperti perbuatan melawan hukum (*actus reus*) yaitu perbuatan yang dilakukan oleh pelaku bertentangan dengan hukum, sifat melawan hukum yaitu perbuatan tersebut harus benar-benar dilarang oleh hukum, Kualitas pelaku yaitu pelaku haruslah seseorang yang memenuhi kriteria tertentu yang diatur oleh hukum untuk dapat dimintai pertanggungjawaban.⁹

Menurut Moeljatno, tindak pidana memiliki dua unsur utama, yaitu unsur formal yang terdiri dari perbuatan (*actie*) dan larangan (*verbod*). Unsur ini merujuk pada suatu perbuatan yang dilarang oleh hukum. Selanjutnya unsur materiil yaitu meliputi perbuatan melawan hukum (*wederrechtelijkheid*) dan akibat yang ditimbulkan (*gevolg*). Unsur ini merujuk pada dampak atau akibat dari perbuatan yang dilarang. Unsur-unsur ini bisa bersifat subjektif atau objektif, tergantung pada apakah mereka berkaitan dengan kondisi batin pelaku (subjektif) atau dengan keadaan di luar pelaku (objektif).¹⁰

⁹ Putri Afifah Yushalia Faisal, *Tinjauan Yuridis Tindak Pidana Memindahkan atau Mentransfer Informasi Elektronik dan/atau Dokumen Elektronik Milik Pemerintah Secara Melawan Hukum (Studi Putusan No. 527/Pid.Sus/2020/Pn.Smn)*, Skripsi, Universitas Hasnuddin, 2022, 15.

¹⁰ M Arif Sahlepi. "Tinjauan Yuridis Terhadap Tindak Pidana Penipuan Secara Online Di Tinjau Dari Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik". *Innovative: Journal Of Social Science Research*, vol. 3, no. 6, Nov. 2023, 1408.

Tindak pidana mengalami perkembangan berdasarkan jenis dan bentuknya seiring perkembangan zaman. Salah satunya yaitu tindak pidana kejahatan di bidang teknologi informasi dengan basis computer.

Tindak pidana kejahatan di bidang teknologi informasi dengan basis computer memiliki beberapa istilah, seperti *computer misuse*, *computer abuse*, *computer fraud*, dan *cybercrime*. Istilah yang sering digunakan oleh PBB adalah *computer-related crime*, sementara istilah *cybercrime* digunakan dalam Konvensi Internasional 2001. *Cybercrime* dapat didefinisikan sebagai tindakan melawan hukum yang merugikan dan memanfaatkan teknologi komputer dan internet. Kejahatan siber mencakup tindakan yang dilakukan secara *offline*, *semi-online*, dan *online*. Sementara itu, Jenis-jenis kejahatan dunia maya meliputi kejahatan murni, kejahatan abu-abu, dan berbagai jenis berdasarkan sasarannya baik itu individu, hak milik, dan pemerintah.

Beberapa contoh kejahatan siber termasuk *defacing*, *unauthorized access*, *illegal contents*, *data forgery*, *cyber espionage*, *cyber sabotage*, dan *offence against intellectual property* memerlukan penanganan dan pemahaman yang mendalam dari para penegak hukum, termasuk para penegak hukum untuk dapat mengatasi kerugian yang ditimbulkannya.

Undang-Undang Nomor 19 Tahun 2016 mendefinisikan sistem elektronik sebagai perangkat dan prosedur yang digunakan untuk mempersiapkan, mengumpulkan, mengolah, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan informasi elektronik. UU ITE (Informasi dan Transaksi

Elektronik) juga mengatur kekuatan hukum serta syarat formil dan materiil dari alat bukti elektronik agar dapat diterima di persidangan. Sistem elektronik ini terkait dengan hukum siber (*cyber law*) yang mencakup berbagai aspek hukum publik dan privat, seperti perlindungan konsumen, anti monopoli, hak kekayaan intelektual, dan *e-commerce*.

Ancaman terhadap sistem elektronik bisa bersifat fisik, seperti kerusakan perangkat keras, gangguan listrik, dan bencana alam, serta non-fisik, seperti serangan *malware*, *DoS (Denial of Service)*, dan pencurian data. Sumber ancaman dapat berasal dari internal organisasi maupun eksternal, termasuk individu, organisasi, dan negara. Bentuk serangan siber mencakup *APT (Advanced Persistent Threat)*, *DoS*, *DDoS (Distributed Denial of Service)*, *defacement*, *phishing*, *malware*, penyusupan siber, spam, dan penyalahgunaan protokol. Penanggulangan serangan siber meliputi langkah-langkah pertahanan siber untuk mengatasi serangan yang mengganggu penyelenggaraan negara, penanganan hukum melalui koordinasi dengan aparat keamanan, dan serangan balik untuk memberikan efek jera kepada pelaku.

Seperti dalam Putusan Nomor 25/Pid.Sus/2019/PN Unh dapat dianalisis secara yuridis terkait tindak pidana yang mengakibatkan terganggunya sistem elektronik telah memenuhi setiap unsur KUHP. Dalam Pasal 49 Jo. Pasal 33 UU RI No.19 Tahun 2016 menunjukkan bahwa Terdakwa L telah dipertanggungjawabkan secara meyakinkan sebagai pelaku dalam kasus ini. Bukti yang diajukan oleh penuntut umum telah menguatkan kesalahan terdakwa L. Selain itu, pengakuan langsung dari Terdakwa

L sendiri dalam persidangan juga menjadikan keabsahannya sebagai pelaku.

Selanjutnya, dalam unsur kesengajaan dan tanpa hak, Terdakwa L dituduh melakukan tindakan yang mengganggu sistem elektronik tanpa hak atau melawan hukum. Ahli hukum pidana mengklasifikasikan kesengajaan menjadi beberapa jenis, yang semuanya relevan dengan kasus ini. Tindakan yang dilakukan Terdakwa L dianggap sebagai kesengajaan dengan pemahaman yang pasti akan konsekuensinya, sesuai dengan Pasal 49 Jo. Pasal 33 UU RI No.19 Tahun 2016. Dengan demikian, analisis ini menunjukkan bahwa Terdakwa L memenuhi unsur-unsur pidana yang didakwakan dengan jelas, sehingga ia harus dipertanggungjawabkan secara hukum sesuai dengan ketentuan yang berlaku.

Perubahan Atas UU RI No.11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. Putusan perkara Nomor 25/Pid.Sus/2019/PN Unh menyatakan bahwa Terdakwa L secara sah dan meyakinkan terbukti bersalah atas tuduhan melakukan tindak pidana dengan sengaja dan tanpa hak, yang mengakibatkan gangguan pada sistem elektronik dan meniadakan fungsi sistem tersebut.

Pidana pokok yang dijatuhkan kepada Terdakwa L adalah penjara selama 1 tahun 4 bulan. Hakim dalam putusannya memiliki kewenangan untuk mempertimbangkan penurunan masa hukuman atau mengganti hukuman dengan rehabilitasi, mengingat motif Terdakwa L yang tidak bermaksud merugikan secara signifikan.

Tuntutan penuntut umum menyatakan bahwa Terdakwa L terbukti secara sah melakukan perbuatan sebagaimana didakwa dalam Pasal 49 Jo. Pasal 33 UU No.19 Tahun 2016, dan menuntut pidana penjara selama 2 tahun, dikurangi masa penahanan sementara. Barang bukti yang diajukan, seperti *screenshot*, flashdisk, handphone, dan laptop, diambil sebagai dasar pemidanaan. Terdakwa L juga diminta untuk membayar biaya perkara sejumlah Rp5.000,-. Dengan demikian, Terdakwa L secara yuridis terbukti melanggar hukum dan harus bertanggung jawab sesuai dengan ketentuan yang berlaku dalam hukum ITE.

Dalam analisis penulis, apa yang disampaikan atau dicantumkan dalam kronologis tindak pidana tersebut baik melalui surat dakwaan, tuntutan, bahkan bukti-bukti yang ditemukan adalah telah sesuai dan memenuhi unsur yuridis dalam surat dakwaan primer. Terdakwa L dalam persidangannya tidak dapat membuktikan adanya alasan pembenar atau alasan pemaaf yang dapat menghapuskan pertanggungjawaban pidananya.

Oleh karena itu, berdasarkan fakta-fakta yang terungkap dalam persidangan dan kesesuaiannya dengan unsur-unsur tindak pidana yang didakwakan, Terdakwa L harus dinyatakan terbukti secara sah dan meyakinkan bersalah melakukan tindak pidana sebagaimana diatur dalam Pasal 49 Jo. Pasal 33 Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik namun menurut teori keseimbangan pemidanaan, hukuman yang diberikan harus proporsional

dengan kejahatan yang dilakukan agar tetap menjaga keadilan bagi semua pihak terkait.¹¹

Pemidanaan Terdakwa L, yang melakukan aksi *defacing* terhadap situs web Pengadilan Negeri Unaaha atas dasar hobi pribadi, dengan pidana 1 tahun 4 bulan, masih dianggap seimbang dalam konteks perundang-undangan yang berlaku. Meskipun demikian, hakim disarankan untuk mempertimbangkan opsi lain yang lebih fokus pada rehabilitasi dalam pengambilan keputusan.

¹¹ Pasal 49 Jo. Pasal 33 Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik

BAB V

PENUTUP

A. Simpulan

Berdasarkan hasil penelitian dan pembahasan di atas maka disimpulkan sebagai berikut, yaitu:

1. Berdasarkan pertimbangan hukum hakim dalam putusan Pengadilan Negeri Nomor 25/Pid.Sus/2019/PN Unh, keputusan yang dihasilkan menegaskan bahwa terdakwa melakukan perbuatan yang terbukti secara sah dan meyakinkan, sebagaimana didakwakan dalam dakwaan Kesatu Primair Pasal 49 Jo. Pasal 33 UU RI Nomor 19 Tahun 2016 tentang Perubahan Atas UU RI Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dan terdakwa secara sah dan meyakinkan terbukti bersalah karena telah memenuhi unsur-unsur sebagai berikut:
 - 1) Unsur setiap orang
 - 2) Unsur sengaja dan tanpa hak atau melawan hukum melakukan tindakan apapun yang berakibat terganggunya system elektronik dan/atau mengakibatkan system elektronik menjadi tidak bekerja sebagaimana mestinya.

Hakim menyatakan bahwa unsur-unsur tindak pidana tersebut terpenuhi, termasuk keberadaan terdakwa yang sesuai dengan surat dakwaan, pengakuan dari terdakwa sendiri, dan dampak yang diakibatkannya terhadap sistem elektronik Pengadilan Negeri Unaaha. Dalam menjatuhkan putusan, hakim mempertimbangkan keadaan yang memberatkan, seperti gangguan berkelanjutan pada akses situs/website pengadilan, serta keadaan yang

meringankan, yakni Kerjasama terdakwa dalam proses persidangan dan catatan hukumnya yang bersih sebelumnya. Putusan ini mencerminkan pertimbangan hukum yang matang, sesuai dengan ketentuan perundang-undangan yang berlaku, serta memastikan keadilan dan kepastian hukum bagi semua pihak yang terlibat.

2. Berdasarkan hasil analisis kasus tindak pidana yang berakibat terganggunya sistem elektronik dalam Putusan Pengadilan Nomor 25/Pid.Sus/2019/PN Unh, terbukti bahwa Terdakwa L melakukan defacing terhadap situs web Pengadilan Negeri Unaha dengan sengaja dan tanpa hak, sesuai dengan Pasal 49 Jo. Pasal 33 Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik. Bukti yang ditemukan, seperti *screenshot*, flashdisk, handphone, dan laptop, menjadi dasar utama dalam penentuan kesalahannya. Hakim menjatuhkan pidana penjara selama 1 tahun 4 bulan dengan mempertimbangkan motif tindakan yang tidak bermaksud merugikan secara signifikan, tetapi tetap memastikan bahwa hukuman yang diberikan sesuai dengan proporsionalitas kejahatan yang dilakukan. Putusan ini menggarisbawahi pentingnya keamanan sistem elektronik dalam konteks hukum digital saat ini dan menunjukkan konsistensi pengadilan dalam memberlakukan hukuman yang adil dan sesuai dengan ketentuan perundang-undangan yang berlaku.

B. Saran

Berdasarkan hasil penelitian di atas, secara umum Undang-undang Nomor 19 Tahun 2016 tentang Perubahan

Atas Undang-undang RI Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sudah cukup mengakomodir ketentuan yang belum ada pada Undang-undang sebelumnya seperti KUHP, KUHPA, Undang-undang tentang telekomunikasi dan sebagainya. Namun ada beberapa hal sebagai bahan evaluasi dan saran antara lain:

1. Bagi Pengguna Internet:

- Meningkatkan kesadaran tentang pentingnya menjaga keamanan *system* elektronik dan data pribadi
- Hendaknya pengguna Internet mematuhi norma dan etika di dunia maya dan tidak melanggar undang-undang yang berlaku, karena jika melanggar Undang-undang maka dapat dikategorikan sebagai tindak kejahatan yang terdapat sanksi hukum bagi yang melanggar

2. Bagi Pemerintah

- Hendaknya pemerintah meningkatkan system pengamanan jaringan computer nasional dan meningkatkan pemahaman serta keahlian aparatur Negara mengenai upaya pencegahan, investigasi dan penuntutan perkara-perkara yang berhubungan dengan kejahatan *cyber*
- Pemerintah perlu meningkatkan kerjasama antar instansi terkait dalam upaya pencegahan dan pemberantasan tindak pidana *cyber*.

DAFTAR PUSTAKA

Buku

- Abidin Farid, Zainal, *Hukum Pidana I*, (Jakarta, Sinar Grafika, 2007).
- Abidin, Zainal, *Pemidanaan, Pidana dan Tindakan Dalam Rancangan KUHP 2005*. (Jakarta, Elsam, 2005)
- Abidin, Zainal, *Pemidanaan, Pidana dan Tindakan dalam Rancangan KUHP 2005*, (Jakarta: ELSAM, 2005).
- Ali, M., *Dasar-dasar Hukum Pidana*, (Jakarta: Sinar Grafika, 2011).
- Ali, Zainudin, *Metode Penelitian Hukum*. (Jakarta: Sinar Grafika, 2014).
- Ariman Rasyid, Raghil Fahmi, *Hukum Pidana*, (Malang, Setara Press, 2015).
- Ariman, R., & Raghil, F., *Hukum Pidana*, (Malang: Setara Press, 2015).
- Arto, Mukti, *Praktek Perkara Perdata pada Pengadilan Agama*, (Yogyakarta, Pustaka Pelajar, 2004)
- Chazawi Adam, *Tindak Pidana Informasi dan Transaksi Elektronik*, (Malang, Media Nusa Creative, 2015).

- Chazawi, A. *Pelajaran Hukum Pidana Bagian I*, Jakarta: PT Raja Grafindo, 2005).
- Darmawan, Deni, Hendra Permana Deden. *Desain dan Pemrograman Website*. (Bandung: PT Remaja Rosdakarya, 2013).
- Effendi, Jonaedi. *Cepat & Mudah Memahami Hukum Pidana*. (Jakarta, Prenada Media, 2016).
- Farid, Zainal Abidin. (2007). *Hukum Pidana I*. Jakarta: Sinar Grafika.
- Hamzah Andi, *Bunga Rampai Hukum Pidana dan Acara Pidana*, (Jakarta, Ghalia Indoensia, 2001).
- Ishaq, *Hukum Pidana*, (Depok: Rajawali Pers, 2020).
- Lamintang, P.A.F., and Franciscus Theojunior Lamintang, *Dasar-Dasar Hukum Pidana Di Indonesia*, 2nd edn (Jakarta: Sinar Grafika, 2016)
- Mahmud Marzuki, Peter, *Penelitian Hukum*, (Jakarta: Kencana, 2005)
- Mahrus Ali, *Dasar Dasar Hukum Pidana*, (Jakarta Sinar Grafika, 2011).

- Maksun, *Kejahatan Siber Cyber Crime: Suatu Pengantar*, (Jakarta: Kencana, 2013).
- Muhammad, Nurul Irfan. *Tindak Pidana Korupsi di Indonesia Dalam Perspektif Fiqh Jinayah*, (Jakarta: Badan Litbang dan Diklat Departemen Agama RI, 2009).
- Nawawi Arief, Barda. (2001). *Masalah penegakan hukum dan kebijakan penanggulangan kejahatan* Bandung, Citra Aditya Bakti.
- Rahardjo Agus, *Cybercrime: Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*, (Bandung, PT Citra Aditya Bakti, 2002).
- Rimdan, *Kekuasaan kehakiman Pasca Amandemen Konstitusi*, (Jakarta: Kencana Prenada Media Group, 2012)
- Rusianto Agus, *Tindak Pidana & Pertanggungjawaban Pidana Tinjauan Kritis Melalui Konsistensi Antara Asas, Teori, Dan Penerapannya*, 1st ed. (Jakarta: Prenadamedia, 2016).
- Rusianto, A. *Tindak Pidana & Pertanggungjawaban Pidana Tinjauan Kritis Melalui Konsistensi antara Asas, Teori, dan Penerapannya*. (Jakarta: Prenadamedia, 2016).

- Sahariyanto, Budi. *Tindak Pidana Teknologi Informasi (Cybercrime): Urgensi Pengaturan dan Celah Hukumnya*. Raja Grafindo Indonesia, 2012.
- Shiefti Dyah Alyusi. *Media Sosial: Interaksi, Identitas, dan Modal Sosial*. (Jakarta: Kencana, 2016).
- Soerjono Soekanto, dkk, *Penelitian Hukum Normative Suatu Tinjauan Singkat*, (Jakarta: Raja Grafindo Persada, 2008).
- Sudikno Mertokusumo, *Mengenal Hukum*, (Liberty, Yogyakarta, 1999), hal 10.
- Sugiyono, *Teori Metode Dasar*, (Jakarta: Gramedia, 2019)
- Suherman, Ade Maman, *Aspek Hukum Dalam Teknologi*, (Jakarta: Ghalia Indonesia, 2002).
- Suyanto, *Pengantar Hukum Pidana*, (Yogyakarta, CV Budi Utama, 2018), hal 68-69.
- Tanhella, dkk., *Buku Ajar Etika Hukum Cyber*, (Magetan: CV AE Media Grafika, 2021), hal 85-87.
- Tere, *Pengertian Sistem Komunikasi: Komponen, Fungsi, dan Jenis-Jenisnya*. (Gramedia Blog, 2020).

- Tofik Yanuar, *Hukum Pidana*, (Jakarta, PT Sangir Multi Usaha, 2022), hal 49-50.
- Wahid Abdul, *Kejahatan Mayantara (Cybercrime)*, (Jakarta: Refika Aditama, 2005).
- Waluyo Bambang, *Pidana dan Pemidanaan*, (Jakarta, Sinar Grafika, 2004)
- Waluyo, Bambang, "*Pidana dan Pemidanaan*", (Jakarta: Sinar Grafika, 2008).
- Widodo, *Aspek Hukum Pidana Kejahatan Mayantara*, (Yogyakarta, Aswaja, 2013), hal 5.
- Yurizal, *Penegakkan Hukum Tindak Pidana Cyber Crime*, (Malang, Media Nusa Creative), hal 16-17.

Jurnal/Skripsi/Artikel

- Aldriano, Anthony. M, Agus Priyambodo. "Cyber Crime Dalam Sudut Pandang Hukum Pidana." *Jurnal Kewarganegaraan* 6.1 (2022): 2170.
- Ayustin, Lani Zihan. *Perbuatan Pidana Mengakses Tanpa Hak Ke Sistem Elektronik Orang Lain Menurut Undang-Undang No. 11 Tahun 2008 Tentang*

Informasi Dan Transaksi Elektronik. Jurnal Ilmiah Mahasiswa Hukum [JIMHUM] 2.3, 2022.

Dachlan, A. *Analisis Hukum Pidana Islam dan HAM Terhadap Hak Korban dan Saksi Dalam Undang-Undang Nomor 12 Tahun 2022 Tentang Tindak Pidana Kekerasan Seksual*. Semarang: Skripsi Universitas Islam Negeri Walisongo, 2022, 40-41 .

Efendi, Firman Yogi, *Analisis Tindak Pidana Cracking Menurut Hukum Positif dan Hukum Pidana Islam*, skripsi Universitas Islam Negeri Walisongo, Semarang, 2020.

Faisal Putri Afifah Yushalia, 2023, *Tinjauan Yuridis Tindak Pidana Memindahkan atau Mentransfer Informasi Elektronik dan/atau Dokumen Elektronik Milik Pemerintah Secara Melawan Hukum (Studi Putusan No. 527/Pid.Sus/2020/Pn.Smn, Skripsi, Universitas Hasanuddin, 2022.*

Arif Sahlepi Muhammad, 2023, Tinjauan Yuridis Terhadap Tindak Pidana Penipuan Secara Online Di Tinjau Dari Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik, *Innovative: Journal Of Social Science Research*, vol. 3, no. 6, Nov. 2023, 1408.

- Muyasir, Ahmad. *Kejahatan Defacing (Perbandingan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik Dan Hukum Pidana Islam)*. Diss. UIN Sunan Kalijaga Yogyakarta, 2015.
- Najib, Chairuddin M. Ade. *Sanksi Terhadap Tindak Pidana Defacing Dalam Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi Dan Tansaksi Elektronik Dengan Prespektif Hukum Islam*. Diss. UIN Raden Fatah Palembang, 2018.
- Pakaya, Usman. “Bahasa Hukum Dalam Putusan Perkara Pidana”, *Negara Hukum* vol. 8, no. 1 (2017), 158.
- Rahayu, Hartoto Suci, *Tinjauan Yuridis Tindak Pidana Defacing Dalam Prespektif Hukum Pidana Di Indonesia (Studi Putusan Pengadilan Negeri Surakarta Nomor 399/Pid.Sus/2017/Pn.Skt)*, skripsi Universitas Sebelas Maret, Surakarta, 2021.
- Setiawan, Beni. *Penegakkan Hukum Pidana Terhadap Akses Sistem Komputer Secara Ilegal (Hacking) Dan Menimbulkan Kejahatan Dunia Maya (Cybercrime) Menurut Prespektif Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi*

Dan Transaksi Elektronik . Diss. Universitas Batanghari, 2019.

Tasya, Yuli, *Cracking Dalam Prespektif Undang-Undang Nomor 11 Tahun 2008 Dan Hukum Pidana Islam*, skripsi Universitas Islam Negeri Sumatera Utara, Medan, 2020.

Krisnawati Valentina Pinky, Edi Pranoto 2023, Tinjauan Yuridis Terhadap Tindak Pidana Elektronik, Vol. 2, No. 1, *Concept: Journal of Social Humanities and Education*, vol. 2, no. 1, Mar. 2023, 60.

Sari, Yolanda, dkk 2022, Analisis Yuridis Terhadap Tindak Pidana Manipulasi Informasi Pengguna E-Commerce Menurut Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik Studi Putusan No. 542/Pid.Sus/2019/PN. Mlg, Vol.2, No.2 *Locus: Jurnal Konsep Ilmu Hukum*, vol. 2, no. 2, Juni 2022, 59.

Peraturan/Perundang-Undangan

Lampiran Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Lampiran Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik

Peraturan Menteri Pertahanan Republik Indonesia Nomor 32 Tahun 2014 Tentang Pedoman Pertahanan Siber, hal 6-15.

Putusan Nomor 25/Pid.Sus/2019/PN Unh.

Undang Undang Republik Indonesia Nomor 48 Tahun 2009 Tentang Kekuasaan Kehakiman.

Website

Damang, “*Definisi Pertimbangan Hukum*”, http://www.damang.web.id/2011/12/definisi-pertimbangan-hukum_17.html. Diakses 20 April 2024.

https://id.wikipedia.org/wiki/Lokator_Sumber_Seragam

<https://tekno.kompas.com/read/2021/12/21/06540017/8-kasus-peretasan-yang-terjadi-di-indonesia-sepanjang-2021?page=all#page2>.

<https://www.liputan6.com/amp/3065275/ini-daftar-puluhan-situs-web-malaysia-yang-kena-serangan-hacker>.

