KAJIAN KRIMINOLOGI TERHADAP TINDAKAN MENGUBAH TAMPILAN SITUS WEB TANPA IZIN

SKRIPSI

Ditulis Untuk Memenuhi Syarat

Mendapatkan Gelar Sarjana Hukum

Oleh :

M.HAFITZ AKSAL HARAHAP

NPM. 2106200066

FAKULTAS HUKUM

UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA

MEDAN

2025

PENGESAHAN SKRIPSI

Judul	:	KAJIAN KRIMINOLOGI TERHADAP TINDAKAN MENGUBAH TAMPILAN SITUS WEB TANPA IZIN
Nama	:	MUHAMMAD HAFITZ AKSAL HARAHAP
Npm	:	2106200066
Prodi / Bagian	:	Hukum/Hukum Pidana

Skripsi tersebut diatas telah diujikan oleh Dosen Penguji Fakultas Hukum Universitas Muhammadiyah Sumatera Utara pada tanggal 11 Juni 2025.

Dosen Penguji

MIRSA ASTUTI, S.H., M.H **NIDN. 0105016901**	**IBRAHIM NAINGGOLAN, S.H., M.H** **NIDN. 0101017406**	**HARISMAN, S.H., M.H** **NIDN. 0103047302**

Disahkan Oleh :
Dekan Fakultas Hukum UMSU

Assoc. Prof. Dr. FAISAL, S.H. M.Hum.
NIDN: 0122087502

MAJELIS PENDIDIKAN TINGGI PENELITIAN & PENGEMBANGAN PIMPINAN PUSAT MUHAMMADIYAH
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
FAKULTAS HUKUM
Akreditasi Unggul Berdasarkan Keputusan Badan Akreditasi Nasional Perguruan Tinggi No. 174/SK/BAN-PT/Ak.Ppj/PT/III/2024
Pusat Administrasi: Jalan Mukhtar Basri No. 3 Medan 20238 Telp. (061) 6622400 – 66224567 Fax. (061)6625474-6631003
https:// umsu.ac.id rektor@umsu.ac.id umsumedan umsumedan umsumedan umsumedan

Bila menjawab surat ini agar disebutkan Nomor dan tanggalnya

بِسْمِ اللَّهِ الرَّحْمَٰنِ الرَّحِيمِ

BERITA ACARA
UJIAN MEMPERTAHANKAN SKRIPSI SARJANA
BAGI MAHASISWA PROGRAM STRATA I

Panitia Ujian Sarjana Strata-1 Fakultas Hukum Universitas Muhammadiyah Sumatera Utara, dalam Sidangnya yang diselenggarakan pada hari **Rabu**, Tanggal **11 Juni 2025**, Jam 08.30 WIB sampai dengan selesai, setelah Mendengar, Melihat, Memperhatikan, Menimbang:

MENETAPKAN

NAMA	:	**MUHAMMAD HAFITZ AKSAL HARAHAP**
NPM	:	**2106200066**
PRODI / BAGIAN	:	**HUKUM/ HUKUM PIDANA**
JUDUL SKRIPSI	:	**KAJIAN KRIMINOLOGI TERHADAP TINDAKAN MENGUBAH TAMPILAN SITUS WEB TANPA IZIN**

Dinyatakan : (**B+**) Lulus Yudisium Dengan Predikat **Lebih Baik**
( ) Lulus Bersyarat, memperbaiki / Ujian Ulang
( ) Tidak Lulus

Setelah lulus dinyatakan berhak dan berwenang mendapatkan gelar **Sarjana Hukum (S.H)** Dalam Bagian **Hukum Pidana.**

PANITIA UJIAN

Ketua	Sekretaris
Assoc. Prof. Dr. FAISAL, S.H., M.Hum	**Assoc. Prof. Dr. ZAINUDDIN, S.H., M.H**
NIDN. 0122087502	**NIDN. 0118047901**

Anggota Penguji:

1. **MIRSA ASTUTI , S.H., M.H.** 1. .....
2. **IBRAHIM NAINGGOLAN, S.H., M.H** 2. .....
3. **HARISMAN, S.H., M.H** 3. .....

MAJELIS PENDIDIKAN TINGGI PENELITIAN & PENGEMBANGAN PIMPINAN PUSAT MUHAMMADIYAH
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
FAKULTAS HUKUM
Akreditasi Unggul Berdasarkan Keputusan Badan Akreditasi Nasional Perguruan Tinggi No. 174/SK/BAN-PT/Ak.Ppj/PT/III/2024
Pusat Administrasi: Jalan Mukhtar Basri No. 3 Medan 20238 Telp. (061) 6622400 – 66224567 Fax. (061)6625474-6631003
https:// umsu.ac.id rektor@umsu.ac.id umsumedan umsumedan umsumedan umsumedan

Bila menjawab surat ini agar disebutkan Nomor dan tanggalnya

بِسْمِ اللَّهِ الرَّحْمَٰنِ الرَّحِيمِ

PENETAPAN
HASIL UJIAN SKRIPSI MAHASISWA FAKULTAS HUKUM UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA

Berdasarkan Berita Acara Ujian Skripsi yang dilaksanakan pada hari **Rabu** anggal **11 Juni 2025.** Panitia Ujian Skripsi Fakultas Hukum Universitas Muhammadiyah Sumatera Utara, dengan ini menetapkan bahwa :

Nama	:	**MUHAMMAD HAFITZ AKSAL HARAHAP**
NPM	:	**2106200066**
Prodi/Bagian	:	**HUKUM/ HUKUM PIDANA**
Judul Skripsi	:	**KAJIAN KRIMINOLOGI TERHADAP TINDAKAN MENGUBAH TAMPILAN SITUS WEB TANPA IZIN**
Penguji	:	**1. MIRSA ASTUTI, S.H., M.H NIDN. 0105016901** **2. IBRAHIM NAINGGOLAN, S.H., M.H, NIDN. 0101017406** **3. HARISMAN, S.H., M.H. NIDN. 0103047302**

Lulus, dengan nilai **B+**, Predikat **Lebih Baik**

Oleh karenanya dinyatakan berhak menggunakan gelar **Sarjana Hukum (S.H)**.

Ditetapkan di Medan
Tanggal, 11 Juni 2025

PANITIA UJIAN

Ketua	**Sekretaris**
Assoc. Prof. Dr. FAISAL, S.H.M.Hum.	**Assoc. Prof. Dr. ZAINUDDIN, S.H.,M.H**
NIDN: 0122087502	**NIDN: 0118047901**

MAJELIS PENDIDIKAN TINGGI PENELITIAN & PENGEMBANGAN PIMPINAN PUSAT MUHAMMADIYAH
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
FAKULTAS HUKUM
Akreditasi Unggul Berdasarkan Keputusan Badan Akreditasi Nasional Perguruan Tinggi No. 174/SK/BAN-PT/Ak.Ppj/PT/III/2024
Pusat Administrasi: Jalan Mukhtar Basri No. 3 Medan 20238 Telp. (061) 6622400 – 66224567 Fax. (061)6625474-6631003
https:// umsu.ac.id rektor@umsu.ac.id umsumedan umsumedan umsumedan umsumedan

Bila menjawab surat ini agar disebutkan Nomor dan tanggalnya

بِسْمِ اللَّهِ الرَّحْمَٰنِ الرَّحِيمِ

PENDAFTARAN UJIAN SKRIPSI

Pendaftaran Skripsi Sarjana Strata 1 Fakultas Hukum Universitas Muhammadiyah Sumatera Utara, Bagi:

NAMA	:	**MUHAMMAD HAFITZ AKSAL HARAHAP**
NPM	:	**2106200066**
PRODI/BAGIAN	:	**HUKUM/ HUKUM PIDANA**
JUDUL SKRIPSI	:	**KAJIAN KRIMINOLOGI TERHADAP TINDAKAN MENGUBAH TAMPILAN SITUS WEB TANPA IZIN**
PENDAFTARAN	:	**TANGGAL, 11 Mei 2025**

Dengan diterimanya Skripsi ini, sesudah lulus dari Ujian Skripsi Penulis berhak memakai gelar:

SARJANA HUKUM (S.H)

Diketahui

DEKAN FAKULTAS HUKUM	**DOSEN PEMBIMBING**
Assoc. Prof. Dr. FAISAL, S.H.,M.Hum.	**HARISMAN, S.H., M.H**
NIDN. 0122087502	**NIDN. 0103047302**

MAJELIS PENDIDIKAN TINGGI PENELITIAN & PENGEMBANGAN PIMPINAN PUSAT MUHAMMADIYAH
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
FAKULTAS HUKUM
Akreditasi Unggul Berdasarkan Keputusan Badan Akreditasi Nasional Perguruan Tinggi No. 174/SK/BAN-PT/Ak.Ppj/PT/III/2024
Pusat Administrasi: Jalan Mukhtar Basri No. 3 Medan 20238 Telp. (061) 6622400 – 66224567 Fax. (061)6625474-6631003
https:// umsu.ac.id rektor@umsu.ac.id umsumedan umsumedan umsumedan umsumedan

Bila menjawab surat ini agar disebutkan Nomor dan tanggalnya

بِسْمِ اللَّهِ الرَّحْمَٰنِ الرَّحِيمِ

BUKTI PENDAFTARAN UJIAN SKRIPSI

Panitia Ujian Skripsi Fakultas Hukum Universitas Muhammadiyah Sumatera Utara telah menerima Pendaftaran Ujian Skripsi:

Nama	:	**MUHAMMAD HAFITZ AKSAL HARAHAP**
NPM	:	**2106200066**
Prodi/Bagian	:	**HUKUM/ HUKUM PIDANA**
Judul Skripsi	:	**KAJIAN KRIMINOLOGI TERHADAP TINDAKAN MENGUBAH TAMPILAN SITUS WEB TANPA IZIN**
Dosen Pembimbing	:	**HARISMAN, S.H., .M.H** **NIDN. 0103047302**

Selanjutnya layak untuk diujiankan

Medan, 11 Mei 2025

PANITIA UJIAN

Ketua	Sekretaris
Assoc. Prof. Dr. FAISAL, S.H. M.Hum.	**Assoc. Prof. Dr. ZAINUDDIN, S.H., M.H**
NIDN. 0122087502	**NIDN. 0118047901**

MAJELIS PENDIDIKAN TINGGI PENELITIAN & PENGEMBANGAN PIMPINAN PUSAT MUHAMMADIYAH
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
FAKULTAS HUKUM
Akreditasi Unggul Berdasarkan Keputusan Badan Akreditasi Nasional Perguruan Tinggi No. 174/SK/BAN-PT/Ak.Ppj/PT/III/2024
Pusat Administrasi: Jalan Mukhtar Basri No. 3 Medan 20238 Telp. (061) 6622400 – 66224567 Fax. (061)6625474-6631003
https:// umsu.ac.id rektor@umsu.ac.id umsumedan umsumedan umsumedan umsumedan

Bila menjawab surat ini agar disebutkan Nomor dan tanggalnya

بِسْمِ اللَّهِ الرَّحْمَٰنِ الرَّحِيمِ

LEMBAR PERSETUJUAN PEMBIMBING

NAMA	:	**MUHAMMAD HAFITZ AKSAL HARAHAP**
NPM	:	**2106200066**
PRODI/BAGIAN	:	**HUKUM/ HUKUM PIDANA**
JUDUL SKRIPSI	:	**KAJIAN KRIMINOLOGI TERHADAP TINDAKAN MENGUBAH TAMPILAN SITUS WEB TANPA IZIN**

Disetujui untuk disampaikan kepada
Panitia Ujian Skripsi

Medan, 23 April 2025

Dosen Pembimbing

HARISMAN, S.H., M.H
NIDN. 0103047302

MAJELIS PENDIDIKAN TINGGI PENELITIAN & PENGEMBANGAN PIMPINAN PUSAT MUHAMMADIYAH
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
FAKULTAS HUKUM
Akreditasi Unggul Berdasarkan Keputusan Badan Akreditasi Nasional Perguruan Tinggi No. 174/SK/BAN-PT/Ak.Ppj/PT/III/2024
Pusat Administrasi: Jalan Mukhtar Basri No. 3 Medan 20238 Telp. (061) 6622400 – 66224567 Fax. (061)6625474-6631003
https:// umsu.ac.id rektor@umsu.ac.id umsumedan umsumedan umsumedan umsumedan

Bila menjawab surat ini agar disebutkan Nomor dan tanggalnya

PERNYATAAN KEASLIAN PENELITIAN

Saya mahasiswa Fakultas Hukum Universitas Muhammadiyah Sumatera Utara yang bertandatangan di bawah ini :

NAMA : **MUHAMMAD HAFITZ AKSAL HARAHAP**

NPM : **2106200066**

PRODI/BAGIAN : **HUKUM/ HUKUM PIDANA**

JUDUL SKRIPSI : **KAJIAN KRIMINOLOGI TERHADAP TINDAKAN MENGUBAH TAMPILAN SITUS WEB TANPA IZIN**

Dengan ini menyatakan sesungguhnya bahwa Skripsi yang saya tulis secara keseluruhan adalah hasil penelitian karya saya sendiri, kecuali pada bagian-bagian yang dirujuk sumbernya. Apabila ternyata di kemudian hari skripsi ini diketahui merupakan hasil plagiat atau merupakan karya orang lain, maka dengan ini saya menyatakan bersedia menerima sanksi akademik sesuai dengan ketentuan yang berlaku.

Medan, 11 Juni 2025

Saya yang menyatakan,

MUHAMMAD HAFITZ AKSAL HARAHAP

NPM. 2106200066

MAJELIS PENDIDIKAN TINGGI PENELITIAN & PENGEMBANGAN PIMPINAN PUSAT MUHAMMADIYAH
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
FAKULTAS HUKUM
Akreditasi Unggul Berdasarkan Keputusan Badan Akreditasi Nasional Perguruan Tinggi No. 174/SK/BAN-PT/Ak.Ppj/PT/III/2024
Pusat Administrasi: Jalan Mukhtar Basri No. 3 Medan 20238 Telp. (061) 6622400 – 66224567 Fax. (061)6625474-6631003
https:// umsu.ac.id rektor@umsu.ac.id umsumedan umsumedan umsumedan umsumedan

KARTU BIMBINGAN SKRIPSI

Nama : M. HAFITZ AKSAL HARAHAP
NPM : 2106200066
Prodi/Bagian : HUKUM/ HUKUM PIDANA
Judul Skripsi : KAJIAN KRIMINOLOGI TERHADAP TINDAKAN MENGUBAH TAMPILAN SITUS WEB TANPA IZIN
Pembimbing : HARISMAN, S.H., M.H

No.	TANGGAL	MATERI BIMBINGAN	TANDA TANGAN
1	16/2 - 2025	Bimbingan judul skripsi	
2	18/2 - 2025	Bimbingan Rumusan masalah	
3	30/2 - 2025	Revisi Bab II	
4	2/3 - 2025	Revisi Bab IV	
5	4/3 - 2025	Rapikan spasi	
6	9/3 - 2025	Rapikan spasi	
7	12/3 : 2025	Perbaiki Footnote	
8	14/3 : 2025	perbaiki daftar Pustaka	
9	23/4-2025	ACC disidangkan	

Mahasiswa dengan data dan judul Tugas Akhir (Jurnal) tersebut di atas telah melalui proses bimbingan dan telah dilakukan pemeriksaan terhadap daftar pustaka, oleh karenanya Tugas Akhir (Jurnal) tersebut disetujui untuk diujiankan.

Diketahui,
Dekan Fakultas Hukum

Assoc. Prof. Dr. FAISAL, S.H., M.Hum
NIDN : 0122087502

Dosen Pembimbing

HARISMAN, S.H., M.H
NIDN : 0103047302

ABSTRAK

KAJIAN KRIMINOLOGI TERHADAP TINDAKAN MENGUBAH TAMPILAN SITUS WEB TANPA IZIN

M.Hafitz Aksal Harahap

Defacing merupakan bentuk kata benda dari kata kerja deface yang artinya merusakkan, mencemarkan, menggores, menghapus. Akan tetapi pengguna istilah ini dalam hukum cybercrime diidentikkan sebagai sebuah kegiatan mengubah tampilan halaman utama atau halaman lain dari suatu website. Sementara itu, dampak yang ditimbulkan dari adanya kejahatan defacing sangat merugikan pemilik website. Serangan defacing yang dilancarkan oleh attacker. Apabila tindak pidana defacing tidak diselesaikan dengan tepat dan tegas maka masyarakat sebagai pengguna dan pemilik website akan semakin resah. Tidak adanya perlindungan baik secara hukum maupun teknis kepada server situs web, akan membuat pihak-pihak yang terlibat dalam kegiatan maya di website menjadi tidak nyaman dan aman. Padahal penggunaan website untuk saat ini dan kedepannya sangat dibutuhkan

Penelitian ini adalah penelitian hukum Yuridis Normatif yang dilakukan dengan cara mengkaji tentang hukum sebagai norma, aturan, asas hukum, prinsip hukum, doktrin hukum, teori hukum, yang kemudian dihubungkan dengan permasalahan yang akan dibahas dalam skripsi ini. pendekatan penelitian ini menggunakan pendekatan Perundang-Undangan, Konseptual dan Kasus.

Pelaku tindakan deface web seringkali mengincar website yang memiliki celah dan kelemahan dalam keamanannya, peretas akan menggunakan berbagai teknik penyerangan untuk melakukan eksploitasi kelemahan ataupun celah dalam keamanan website Adapun Faktor terjadinya defacing adalah faktor Internal dan Eksternal. hactivism, yaitu aktivitas yang dilakukan oleh hacker, defacing hanyalah salah satu bentuk dari hactivism itu. Defacing merupakan aktivitas modification; dalam arti tindakan melakukan perubahan terhadap data atau informasi atau konten yang mengalir dalam sebuah infrastruktur teknologi informasi tanpa sepengetahuan yang mengirimkan atau menerimanya. Upaya penanggulangan kejahatan telah dan terus dilakukan oleh semua pihak, baik pemerintah maupun masyarakat pada umumnya. Berbagai program dan kegiatan telah dilaksanakan sambil terus mencari cara tepat dan efektif untuk mengatasi masalah tersebut. upaya penanggulangan kejahatan mencakup aktivitas preventif sekaligus berupaya memperbaiki prilaku seseorang dinyatakan telah bersalah (terpidana) di Lembaga Pemasyarakatan atau dengan kata lain, upaya kejahatan dapat dilakukan secara pre-emptif, preventif dan represif

Kata Kunci : Kriminologi, Mengubah Tampilan, Tanpa Izin.

DAFTAR ISI

BAB I

PENDAHULUAN

A. Latar Belakang

Teknologi informasi (*information technology*) memegang perananyang penting, baik di masa kini maupun nanti. Teknologi informasi sangat diyakini akan membawa keuntungan dan kepentingan yang begitu besar untuk semua negara-negara yang ada di dunia. Setidaknya ada 2 (dua) hal yang membuat teknologi informasi dianggap begitu penting dalam memacu pertumbuhan ekonomi dunia, yaitu:

1. Teknologi informasi mendorongpermintaan atas produk-produk teknologi informasi itu sendiri, seperti: komputer, modem, sarana untuk membangun jaringan internet dan sebagainya.
2. Untuk memudahkan transaksi bisnis terutama bisnis keuangan di samping bisnis-bisnis umum lainnya.[1]

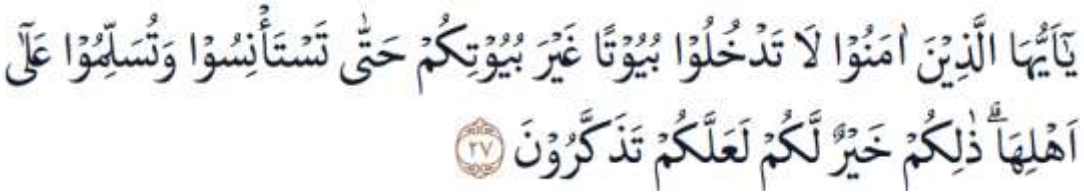
Kemajuan ilmu pengetahuan dan teknologi telah mempengaruhi pola pikir dan gaya hidup masyarakat menuju ke era modern. Teknologi pada dasarnya diciptakan untuk peningkatan kualitas hidup dan mempermudah aktivitas manusia menjadi lebih efektif dan efisien. Namun tidak dapat dipungkiri bahwa teknologi selain memiliki sisi positif, juga memiliki sisi negatif. Dalam berbagai kajian penelitian, kemajuan teknologi menunjukkan korelasi yang positif dengan meningkatnya kriminalitas. Sikap ketergantungan, keteledoran, kekurangpahaman

[1] Grace Yurico Bawole,(2013) "Kajian Yuridis Terhadap Perlindungan Pemilik Website Dalam Upaya Pencegahan dan Penanggulangan Kriminalisasi Cyber Crime di Indonesia", Lex Crimen Vol. 2, No. 3, halaman 64.

atau kesengajaan dalam menggunakan komputer akan menimbulkan dampak negatif, bilamana tidak diimbangi dengan sikap mental dan sikap tindak positif.[2]

Internet atau media sosial *online* adalah sebuah sistem komunikasi global yang menghubungkan berbagai komputer dengan sebuah jaringan di seluruh dunia yang disebut *network.* Cara menghubungkan komputer ke media sosial *online* yaitu memanfaatkan layanan dari perusahaan penyedia akses media sosial *online*, yang disebut ISP (*internet service provider*). Dengan adanya ISP, maka komputer dapat berhubungan dan bertukar data dengan komputer lain di seluruh dunia.[3]

Dalam konteks keislaman, Al-Quran tidak membatasi umat islam untuk melakukan kemajuan, justru islam sangat mengutamakan agar manusia senantiasa melakukan *research* guna keperluan ilmu pengetahuan, salah satunya dalam ranah pengetahuan dan pengembangan teknologi. Dalam islam, teknologi merupakan bagian dari ayat-ayat Allah SWT yang perlu digali dan dicari kebenarannya, Islam juga menghormati hak Pribadi atau *Privacy* seseorang seperti dalam QS An-Nur ayat 27:


يَٰٓأَيُّهَا ٱلَّذِينَ ءَامَنُوا۟ لَا تَدْخُلُوا۟ بُيُوتًا غَيْرَ بُيُوتِكُمْ حَتَّىٰ تَسْتَأْنِسُوا۟ وَتُسَلِّمُوا۟ عَلَىٰٓ
أَهْلِهَا ۚ ذَٰلِكُمْ خَيْرٌ لَّكُمْ لَعَلَّكُمْ تَذَكَّرُونَ ٢٧

[2] Barda Nawawi Arif. 2012. Kebijakan Integral Penanggulangan Cyberporn di Indonesia. Semarang:Lima, halaman 1.

[3] Harisman, (2015),"Pemanfaatan Media Sosial Online Dalam Mendukung Pembelajaran Sosiologi (Studi Kasus Kelas XI IPS)", Thesis Diploma, FIS, halaman 12.

Artinya: *"Hai orang-orang yang beriman, janganlah kamu memasuki rumah yang bukan rumahmu sebelum meminta izin dan memberi salam kepada penghuninya. Yang demikian itu lebih baik bagimu, agar kamu (selalu) ingat"*. (An-Nur ayat 27).

Sistem hukum pidana Indonesia, tidak ada definisi eksplisit tentang kejahatan dunia maya yang diuraikan dalam undang-undang. Sebaliknya, fokusnya adalah pada tindakan pidana yang terkait dengan teknologi informasi dan transaksi elektronik sebagaimana dimaksud dalam UU ITE. Kejahatan dunia maya mencakup berbagai kegiatan, mulai dari akses tidak sah ke sistem komputer hingga pencurian data dan vandalisme jahat.

Kejahatan dunia maya menimbulkan ancaman yang signifikan terhadap stabilitas masyarakat Indonesia, yang menantang kemampuan pemerintah untuk memerangi kejahatan yang dilakukan melalui teknologi komputer, terutama melalui jaringan internet dan intranet. Seiring dengan pesatnya perkembangan teknologi, kejahatan dunia maya pun berkembang pesat, dengan para pelaku memanfaatkan dunia maya untuk melakukan kegiatan ilegal.[4]

Kejahatan dunia maya antara "*virtual crime*" atau cyber crime sudah terjadi di Indonesia sejak tahun 1983 samapai saat ini dengan cara menyalahgunakan komputer. Komputer adalah alat pemroses data elektronik, magnetik, optikal, atau sistem yang melaksanakan fungsi logika, aritmetika, dan penyimpanan. Barda Nawawi Arief mengemukakan bahwa pengertian kejahatan yang berhubungan dengan komputer sama

[4] Muh. Fadli Faisal Rasyid, *et.al,* (2024),"Cybercrime Threats and Responsibities: The Utilization of Artificial Intelligence in Online Crime", Jurnal Ilmiah Mizani, Vol.11, No.1, halaman 54.

dengan cyber crime. Secara terminologis, kejahatan yang berbasis pada teknologi informasi dengan menggunakan media komputer sebagaimana terjadi saat ini, dapat disebut dengan beberapa istilah yaitu computer misuse, computer abuse, computer fraud, computer related-crime, computer assisted crime, atau computer crime. Namun demikian, setiap negara belum tentu sama dalam menggunkan istilah tersebut, bahkan tidak konsisten.

Kejahatan siber merupakan keseluruhan bentuk kejahatan yang ditujukan terhadap komputer, jaringan komputer dan para penggunanya, dan bentuk-bentuk kejahatan tradisional yang menggunakan atau dengan bantuan komputer.Dapat disimpulkan bahwa kejahatan siber adalah setiap aktivitas seseorang, sekelompok orang, badan hukum yang menggunakan komputer sebagai sarana melakukan kejahatan, dan komputer sebagai sasaran kejahatan.Kejahatan tersebut adalah bentuk-bentuk kejahatan yang bertentangan dengan peraturan perundang-undangan.Indonesia sebagai negara hukum, selalu mengutamakan semua kegiatan kenegaraan dan kemasyarakatan didasarkan pada ketentuan hukum.

Karena hal itu, Indonesia selalu berusaha untuk melakukan pembaharuan Hukum Pidana, salah satunya dengan menerbitkan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE).Karena penyelenggaraan kegiatan dalam bidang teknologi yang berbasis komputer sangat penting bagi masyarakat dan rawan melakukan pelanggaran hak asasi manusia, maka dalam melakukan kriminalisasi, Indonesia dapat memperhatikan himbauan, anjuran, rekomendasi dari Perserikatan Bangsa-Bangsa.Berkaitan dengan kriminalisasi terhadap perbuatan yang berkategori

kejahatan siber (*cyber crime*). PBB sendiri menentukan bahwa ketentuan pidana dalam perbuatan perundang-undangan setiap negara wajib melakukan perumusan ketentuan pidana secara jelas (*lex certa*).Dimana hal ini dilakukan dalam rangka memberikan perlindungan hukum bagi rakyat Indonesia, memberikan kejelasan, menjamin kepastian ketentuan hukum, agar tidak terjadi ambiguitas penafsiran.[5]

Di era digital yang semakin maju, kemajuan teknologi informasi dan komunikasi telah memberikan dampak positif bagi masyarakat global. Namun, pada saat bersamaan, muncul ancaman baru berupa kejahatan dunia maya. Kejahatan yang cukup umum di dunia cyber crime adalah deface website. Deface website merupakan tindakan yang dilakukan oleh seorang hacker atau peretas dengan tujuan untuk merusak atau mengubah tampilan *homepage* sebuah website. Tindakan ini sering terjadi untuk menodai reputasi organisasi atau individu, mengeksploitasi kerentanan dalam dalam sistem keamanan, atau menyampaikan pesan politik atau ideologis. Kejahatan dunia maya berupa perusakan situs web memiliki konsekuensi serius, baik bagi pemilik situs web maupun bagi pengguna yang mengandalkan informasi atau layanan yang dikandungnnya. Selain itu, degradasi situs web juga dapat menjadi titik awal serangan yang lebih berbahaya, seperti pencurian data pribadi atau serangan penolakan layanan.[6] Istilah *defacing* merupakan bentuk kata benda dari kata kerja deface yang artinya merusakkan, mencemarkan, menggores, menghapus. Akan tetapi pengguna

[5] Ibrahim Fikma Edrisky. 2019. Pengantar Hukum Siber. Lampung: Sai Wawai, halaman 3.

[6] Brian Budi Aji, (2023). "Tindakan Kejahatan Cyber Crime Dalam Bentuk Deface Website", Cybersecurity dan Forensik Digital, Vol. 6, No. 1, halaman 25.

istilah ini dalam hukum cybercrime diidentikkan sebagai sebuah kegiatan mengubah tampilan halaman utama atau halaman lain dari suatu website dalam satu url dari website yang bersangkutan baik itu di dalam folder maupun di file. Ketika security dari suatu sistem memiliki celah maka disitulah teknik ini digunakan oleh para *defacer* dalam melancarkan aksinya terhadap aplikasi atau website tersebut. Tujuan tindakan ini adalah untuk mengubah tampilan yang dikehendaki oleh defacer. Adapun tahapan dalam *defacing* terbagi dua tahap pertama adalah dengan melakukan hacking atau menerobos sistem milik orang lain atau publik dan masuk ke dalam web server. Tahap kedua adalah dengan mengubah dan mengganti tampilan web (*web page*).

Sementara itu, dampak yang ditimbulkan dari adanya kejahatan defacing sangat merugikan pemilik website. Serangan defacing yang dilancarkan oleh attacker membuat website menjadi kacau bahkan tidak berfungsi lagi. Layanan website yang awalnya normal menjadi tidak dapat diakses. 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 yang paling mengkhawatirkan adalah defacer memiliki fungsi otoritas di dalam website, akibatnya admin server website beralih ke tangan defacer secara permanen.

Terjadinya kasus defacing melalui dua tahap, yang pertama melakukan hacking terlebih dahulu terhadap website dan tahap selanjutnya mengubah tampilan website

tersebut, Oleh karena itu, dengan dibentuknya Undang-Undang Nomor 11 Tahun 2008 Juncto Undang-Undang No 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik oleh pemerintah diharapkan agar semua kejahatan mayantara dapat terakomodir oleh Undang-Undang tersebut, termasuk defacing yang telah diatur didalamnya yakni pada pasal 30 ayat (1) ayat (2) ayat (3) dan pasal 32 ayat (1) Undang- Undang No 11 Tahun 2008 Juncto Undang-Undang No 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik.

Apabila tindak pidana defacing tidak diselesaikan dengan tepat dan tegas maka masyarakat sebagai pengguna dan pemilik website akan semakin resah. Tidak adanya perlindungan baik secara hukum maupun teknis kepada server situs web, akan membuat pihak-pihak yang terlibat dalam kegiatan maya di website menjadi tidak nyaman dan aman. Padahal penggunaan website untuk saat ini dan kedepannya sangat dibutuhkan terutama guna kepentingan bisnis dan pemerintahan. Jika pemerintah dan penegak hukum tidak bisa memberikan fungsi keamanan bagi pemilik website maupun sistem elektronik atau dokumen elektronik lainnya maka wajar saja para investor lokal maupun asing akan ragu dalam berinvestasi di Indonesia sebab semua aktivitas bisnis ke depan menggunakan layanan berbasis online.

Pada akhirnya, berdasarkan uraian sebagaimana dijelaskan di atas, Penulis membuat judul penelitian berupa "**Kajian Kriminologi Terhadap Tindakan Mengubah Tampilan Situs Web Tanpa Izin"**

1. Rumusan masalah

Berdasarkan uraian sebelumnya, penelitian ini akan membahas permasalahan sebegai berikut:

a. Bagaimana faktor-faktor yang menjadi penyebab terjadinya Tindakan mengubah tampilan situs web tanpa izin?
b. Bagaimana bentuk-bentuk kejahatan terhadap Tindakan mengubah tampilan situs web tanpa izin?
c. Bagaimana upaya penanggulangan Hukum Pidana terhadap Tindakan mengubah tampilan situs web tanpa izin?

2. Tujuan Penelitian

Tujuan penelitian harus tergambar secara tegas apa yang hendak dicapai di dalam melaksanakan penelitian tersebut. Tujuan penelitian harus bertitik tolak dari permasalahan. Bahkan harus terlihat tegas dan konkrit serta relevan.[7] Adapun tujuan dari penelitian ini adalah:

a. Untuk mengetahui faktor-faktor yang menjadi penyebab terjadinya Tindakan mengubah tampilan situs web tanpa izin.
b. Untuk mengetahui bentuk-bentuk kejahatan terhadap Tindakan mengubah tampilan situs web tanpa izin.
c. Untuk mengetahui upaya penanggulangan Hukum Pidana terhadap Tindakan mengubah tampilan situs web tanpa izin.

[7] Faisal, et.al. 2023. *Pedo man Penulisan dan Penyelesaian Tugas Akhir Mahasiswa*. Medan: Pustaka Prima, halaman 5

3. Manfaat Penelitian

Dalam penelitian ini penulis mengharapkan adanya beberapa manfaat yang akan diperoleh sebagai berikut :

a. Secara teoritis, Penelitian ini akan memberikan kontribusi pada pengembangan teori kriminologi, khususnya dalam memahami fenomena kejahatan di dunia maya (cybercrime). Hal ini membuka perspektif baru dalam studi tentang kejahatan digital dan bagaimana tindakan seperti mengubah tampilan situs web tanpa izin dapat dianalisis dari sudut pandang kriminologi.
b. Secara Praktis, Penelitian ini dapat memberikan informasi yang berguna bagi aparat penegak hukum dalam mengidentifikasi dan menangani kasus pengubahan tampilan situs web tanpa izin. Ini juga dapat membantu penegak hukum untuk lebih memahami aspek-aspek teknis dari kejahatan siber ini.

B. Definisi Operasional

Untuk mempermudah penulisan, maka perlu diberikan suatu Batasan pengertian umum terhadap judul penelitian ini, yaitu, **"Kajian Kriminologi Terhadap Tindakan Mengubah Tampilan Situs Web Tanpa Izin".**

1. Kriminologi merupakan suatu ilmu pengetahuan yang mempelajari tentang penjahat dan kejahatan, serta mempelajari cara-cara penjahat melakukan kejahatan, kemudian berusaha semaksimal mungkin untuk mengetahui faktor yang menyebabkan terjadinya kejahatan dan bagaimana upaya untuk

mencari dan menemukan cara untuk dapat mencegah dan menanggulangi terjadinya kejahatan.[8]

2. Mengubah tampilan situs web (*defacing*), merupakan bentuk kata benda dari kata kerja *deface* yang artinya merusakkan, mencemarkan, menggores, menghapus. Akan tetapi pengguna istilah ini dalam hukum *cybercrime* diidentikkan sebagai sebuah kegiatan mengubah tampilan halaman utama atau halaman lain dari suatu website dalam satu url dari website yang bersangkutan baik itu di dalam folder maupun di file.
3. Izin pada hakikatnya merupakan pengecualian terhadap ketentuan larangan. Izin juga dapat diartikan sebagai dispensasi atau pelepasan atau pembebasan dari suatu larangan.[9]

C. Keaslian Penelitian

Penulisan skripsi ini merupakan syarat yang harus dipenuhi untuk memperoleh gelar kesarjanaan di Fakultas Hukum Universitas Muhammadiyah Sumatera Utara. Sepanjang pengetahuan penulis dilingkungan Perpustakaan Fakultas Hukum Universitas Muhammadiyah Sumatera Utara, **"Kajian Kriminologi Terhadap Tindakan Mengubah Tampilan Situs Web Tanpa Izin"** Dari beberapa judul penelitian yang pernah diangkat peneliti sebelumnya, ada dua judul yang hampir mendekati sama dengan penelitian ini, antara lain:

---

[8] Beby Suryani. (2023). *Kriminologi.* Deli Serdang: Universitas Medan Area Press, halaman 3.

[9] Fathoni, S.Tisnanta, (2018), "Konstruksi Makna Izin Sebagai Instrumen Pengadilan Versus Kebijakan Kemudian Investasi Di Provinsi Lampung", Jurnal Hukum Peratun, Vol. 1,No. 1, halaman 84.

1. Lois Laminola Bancin, NIM 1912011026, Fakultas Hukum Universitas Lampung 2023, Yang berjudul "Kajian Kriminologi Terhadap Kejahatan Memindahkan Atau Mentransfer Informasi Elektronik Dan atau Dokumen Elektronik (Studi Putusan Nomor: 527/Pid.Sus/2020/PN Smn)". Bahwa Perbedaan dari penelitian ini adalah terletak pada pembahasan isi dari penelitian, dimana sebelumnya peneliti lebih memfokuskan isi pembahasannya mengenai faktor penyebab terjadinya Kejahatan Memindahkan atau Mentransfer Informasi Elektronik dan atau Dokumen Elektroni sedangkan dalam penulisan penulis lebih memfokuskan. faktor-faktor yang menjadi penyebab terjadinya Tindakan mengubah tampilan situs web tanpa izin Maka berdasarkan keterangan diatas penelitian terdahulu dan sekarang adalah penelitian yang berbeda.
2. Mustakim, NIM 0121.02.46.2017, Fakultas Hukum Universitas Muslm Indonesia Makassar 2019, Yang berjudul "Cyber Crime Dalam Perspektif Kriminologi Kontemporer". Bahwa Perbedaan dari penelitian ini adalah terletak pada pembahasan isi dari penelitian, dimana sebelumnya peneliti lebih memfokuskan isi pembahasannya mengenai n bagaimana cyber crime ditinjau dari perspektif kriminologi kontemporer. sedangkan dalam penulisan penulis lebih memfokuskan. faktor-faktor yang menjadi penyebab terjadinya Tindakan mengubah tampilan situs web tanpa izin Maka berdasarkan keterangan diatas penelitian terdahulu dan sekarang adalah penelitian yang berbeda

3. Adhi Dharma Aryyaguna, NIM B1112358, Fakultas Hukum Universitas Hasnuddin Makassar 2017, Yang berjudul "Tinjauan Kriminologis Terhadap Kejahatan Penipuan Berbasis Online (Studi Kasus Unit Cyber Crime Reskrimsus Polda Sulsel)". Bahwa Perbedaan dari penelitian ini adalah terletak pada pembahasan isi dari penelitian, dimana sebelumnya peneliti lebih memfokuskan isi pembahasannya mengenai Bagaimanakah penanggulangan kejahatan penipuan berbasis online yang dilakukan oleh pihak yang berwenang. sedangkan dalam penulisan penulis lebih memfokuskan. Untuk mengetahui upaya penanggulangan Hukum Pidana terhadap Tindakan mengubah tampilan situs web tanpa izin Maka berdasarkan keterangan diatas penelitian terdahulu dan sekarang adalah penelitian yang berbeda

D. Metode Penelitian

Metode berasal dari kata Yunani "methodos," yang artinya cara atau jalan, Penelitian berasal dari kata "research" yang artinya penelitian atau penyelidikan. Jadi, metodologi penelitian merupakan upaya untuk menyelidiki dan menggali suatu permasalahan dengan menggunakan metode ilmiah secara cermat dan teliti. Tujuan utamanya adalah meraih, mengolah, menganalisis data, dan mencapai kesimpulan secara sistematis dan obyektif.[10] Maka metode penelitian yang dilakukan meliputi:

[10] Tamaulina Br.Sembiring, *et.al.* 2024. *Buku Ajar Metodologi Penelitian (Teori Praktik)*. Karawang: CV Saba Jaya Publisher. Halaman 1.

1. Jenis Penelitian

Penelitian ini menggunakan jenis penelitian yang dilakukan dengan pendekatan yuridis normatif, penelitian hukum normatif adalah proses penelitian untuk meneliti dan mengkaji tentang hukum sebagai norma, aturan, asas hukum, prinsip hukum, doktrin hukum, teori hukum dan kepustakaan lainnya untuk menjawab permasalahan hukum yang diteliti.[11]

2. Sifat Penelitian

Penelitian ini bersifat deskriptif, sifat penelitian deskriptif analitis Yaitu menggambarkan atau mendeskripsikan ketentuan perundang-undangan yang berkaitan mengenai Faktor Motivasi dendam pelaku sebagai kausalitas sebab kematian pada tindak pidana pembunuhan.

3. Pendekatan Penelitian

Pendekatan-pendekatan yang digunakan dalam penelitian hukum ada beberapa pendekatan adalah sebagai berikut ;

a. Pendekatan per-undang-undangan (*statute approach*), Pendekatan ini dilakukan dengan menelaah semua peraturan perundang-undangan dan regulasi yang terkait dengan isu hukum yang sedang bahas (diteliti).
b. Pendekatan konseptual (*conceptual approach*), Pendekatan ini beranjak dari pandangan-pandangan dan doktrin-doktrin yang berkembang dalam

[11] Muhaimin. 2020. *Metode Penelitian Hukum*. Mataram: Mataram University Press. Halaman 48.

ilmu hukum.[12]

4. Sumber Data

Sumber data dari penelitian ini terdiri dari:

a. Data yang bersumber dari hukum islam; yaitu Al-Qur'an dan Hadist. Data yang bersumber dari Hukum Islam tersebut lazim disebut sebagai data kewahyuan, yaitu surat Al-Imran ayat 191;

الَّذِيْنَ يَذْكُرُوْنَ اللّٰهَ قِيَامًا وَّقُعُوْدًا وَّعَلٰى جُنُوْبِهِمْ وَيَتَفَكَّرُوْنَ فِيْ خَلْقِ السَّمٰوٰتِ
وَالْاَرْضِۚ رَبَّنَا مَا خَلَقْتَ هٰذَا بَاطِلًاۚ سُبْحٰنَكَ فَقِنَا عَذَابَ النَّارِ ﴿١٩١﴾

Artinya: *"Hai orang-orang yang beriman, janganlah kamu memasuki rumah yang bukan rumahmu sebelum meminta izin dan memberi salam kepada penghuninya. Yang demikian itu lebih baik bagimu, agar kamu (selalu) ingat"*. (An-Nur ayat 27).

b. Data Primer, yaitu data yang diperoleh melalui bahan pustaka yang terdiri dari:.

1) Bahan hukum primer yaitu bahan hukum yang bersumber dari peraturan perundang-undangan yang mempunyai relevansi yang kuat terhadap objek yang akan diteliti dalam penelitian ini yang terdiri dari Kitab Undang-Undang Hukum Pidana, Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik, Undang-Undang Dasar Negara Republik Indonesia 1945,

[12] *Ibid.,*Halaman 57.

Kitab Undang-Undang Hukum Pidana (KHUP).

2) Bahan hukum sekunder, yaitu bahan yang memberikan penjelasan mengenai bahan hukum primer, berupa publikasi tentang hukum meliputi buku, karya ilmiah jurnal, dan komentar-komentar hukum yang berkaitan dengan permasalahan penelitian.
3) Bahan hukum tersier, yaitu bahan-bahan yang memberi petunjuk maupun penjelasan terhadap bahan hukum primer dan sekunder, seperti: kamus hukum, ensiklopedia, ensiklopedia hukum, kamus Bahasa dan data sensus.[13]

5. Alat Pengumpul Data

Penelitian ini menggunakan alat pengumpul data berupa studi kepustakaan (*library research*). Tenik pengumpulan data dalam penelitian hukum normatif dilakuan dnegan studi pustaka terhadap bahan-bahan hukum, data penelitian yang dikumpulkan dengan cara studi Kepustakaan yaitu mengumpulkan dan memeriksa dokumen-dokumen yang dapat memberikan informasi atau yang dibutuhkan oleh peneliti.[14]

6. Analisis Data

Analisis data dalam penelitian ini menggunakan analisis kualitatif, yaitu dimana data yang diperoleh dalam studi kepustakaan (*library research*) atas bahan hukum akan diuraikan dan dihubungkan sedemikian rupa sehingga dapat disajikan dalam bentuk

[13] Ibid.,halaman 62.
[14] Nur Solikin. 2021. Pengantar Metodologi. Pasuruan: CV. Penerbit Qiara Media. Halaman 119.

penulisan yang lebih sistematis guna mecapai target yang diinginkan. Pengolahan bahan hukum dilakukan secara deduktif, yakni menarik kesimpulan dari suatu permasalahan yang bersifat umum untuk permasalahan yang bersifat konkret yang sedang dihadapi.

BAB II

TINJAUAN PUSTAKA

1. Kriminologi

Kriminologi merupakan suatu ilmu pengetahuan yang mempelajari tentang penjahat dan kejahatan, serta mempelajari cara-cara penjahat melakukan kejahatan, kemudian berusaha semaksimal mungkin untuk mengetahui faktor yang menyebabkan terjadinya kejahatan dan bagaimana upaya untuk mencari dan menemukan cara untuk dapat mencegah dan menanggulangi terjadinya kejahatan. Istilah kriminologi untuk pertama kalinya digunakan oleh P. Topinard (1830- 1911) seorang ahli antropologi Perancis pada tahun 1879, sebelumnya istilah yang banyak dipakai adalah Antropologi Kriminal.[15]

Kriminologi merupakan ilmu pengetahuan yang mempelajari sebab-sebab terjadinya kejahatan yang dilihat dari berbagai segi. Berdasarkan hal tersebut maka kriminologi merupakan pertanyaan MENGAPA dan BAGAIMANA ? artinya mengapa orang melakukan kejahatan dan bagaimana upaya yang harus dilakukan untuk mencegah terjadinya kejahatan. Edwin Sutherland seorang kriminologi Amerika Serikat yang terkemuka menyatakan bahwa dalam mempelajari kriminologi memerlukan bantuan berbagai disiplin ilmu pengetahuan. Dengan kata lain kriminologi merupakan disiplin ilmu yang bersifat interdisipliner. Sultherland menyatakan *criminology is a body of knowledge* (kriminologi adalah kumpulan pengetahuan).

[15] Beby Suryani. *Op.cit*.,halaman 3.

Berbagai disiplin yang sangat erat kaitannya dengan kriminologi antara lain hukum pidana, hukum acara pidana, antropologi pisik, antropologi budaya, psikologi, biologi, ekonomi, kimia, statistik, dan banyak lagi disiplin lainnya yang tidak dapat disebutkan dalam tulisan ini. Lebih lanjut vanBemmelen menyatakan bahwa kriminologi layaknya "*The King Without Countries*" sebab daerah kekuasaannya tidak pernah ditetapkan. Kriminologi mengambil konsep dasar dan metodologinya dari ilmu tingkah laku manusia, biologi, dan nilai-nilai historis serta sosiologis hukum pidana.[16]

Kriminologi diamalkan untuk kepentingan memahami kejahatan dan berbagai perilaku yang menyimpang dan bukanlah sarana yang diterapkan bagi peradilan semata-mata seperti kriminalistik, melainkan sebagai pure science yang hasil penelitiannya secara objektif dapat dimanfaatkan bagi kepentingan praktis. Kriminologi itu suatu gabungan (complex) ilmuilmu lain, yang dapat disebut ilmu bagian (deelwetenschap) dari kriminologi. Kriminologi adalah ilmu yang menyelidiki dan membahas asal-usul kejahatan (etiologi kriminal, criminale aetiologi). Dimana kejahatan dapat dipandang sebagai sesuatu yang bukan hanya pelanggaran hukum saja namun sebagai tindakan manusia dan suatu gejala sosial.[17]

Kriminologi dapat dijelaskan sebagai keseluruhan pengetahuan yang diperoleh berdasarkan teori atau pengalaman yang berkaitan dengan perbuatan jahat dan penjahat dan termasuk reaksi masyarakat terhadap perbuatan jahat dan penjahat tersebut.

---

[16] EmiliaSusanti. *Et al.* 2018. *Hukum dan Kriminologi*. Lampung: Aura, halaman 6.
[17] Ibid., halaman 12.

Kejahatan yang dimaksud adalah tindakan yang dilarang oleh undang-undang. Pemahaman ini memberikan pandangan yang tepat tentang kriminologi sebagai bagian dari ilmu yang mempelajari perilaku kriminal. Kriminologi dibagi menjadi tiga bidang ilmu utama, yaitu:

1. Sosiologi hukum adalah kajian tentang bagaimana tindakan tertentu dianggap sebagai kejahatan berdasarkan norma-norma hukum yang melarangnya dan mengancam dengan sanksi. Oleh karena itu, penentuan apakah suatu tindakan dianggap sebagai tindak kriminal bergantung pada prinsip-prinsip hukum.
2. Etiologi Kriminal adalah bagian dari kriminologi yang bertujuan untuk melakukan analisis ilmiah tentang asal-usul kejahatan
3. Penologi adalah ilmu yang mempelajari hukuman, mencakup penerapan hak-hak yang berkaitan dengan usaha pengendalian kejahatan, baik melalui tindakan represif maupun preventif.[18]

Tindak kejahatan di bidang teknologi informasi sering dikategorikan sebagai white crime karena pelakunya memiliki pemahaman dan keahlian dalam menggunakan aplikasi internet atau bidang terkait. Karena kejahatan ini sering melintasi batas negara dan dilakukan secara transnasional, kejahatan dunia maya ini dapat digolongkan sebagai dua jenis kejahatan, yaitu white crime dan transnational crime.

[18] Muhammad Fadli, Dijan Widijowati, Dwi Andayani, (2024), " Pencurian Data Pribadi di Dunia Maya (Phising Cybercrime) yang ditinjau dalam Prespektif Kriminologi", Co-Value: Jurnal Ekonomi, Koperasi, Kewirausahaan, Vol. 14, No.12, halaman 6.

Dalam sudut pandang kriminologi, ada beberapa faktor dan alasan yang menyebabkan kasus cybercrime terjadi. Dari segi alasan, kejahatan ini biasanya dapat dibagi menjadi dua kategori, yaitu:

1. Motif intelektual kriminal terjadi saat seseorang melakukan kejahatan semata-mata untuk kepuasan pribadi dan untuk menunjukkan kemampuannya dalam merancang dan menerapkan teknologi informasi. Motif ini umumnya dilakukan oleh individu
2. Motif ekonomi, politik, dan kriminalitas merujuk pada alasan di balik suatu tindak kriminal yang dilakukan dengan tujuan memperoleh keuntungan pribadi atau kelompok yang dapat merugikan pihak lain baik secara ekonomi maupun politis. Kriminalitas dengan motif ini, bertujuan untuk menciptakan dampak besar dan sering kali dilakukan oleh perusahaan atau korporasi..[19]

Berdasarkan teori kriminologi, penanganan cybercrime dapat dilihat melalui beberapa perspektif yang membantu memahami dan mengatasi kejahatan siber secara efektif. Yaitu:

1. Teori Pembelajaran Sosial (*Social Learning Theory*)

   Teori Pembelajaran Sosial (*Social Learning Theory*), yang dikemukakan oleh Albert Bandura, juga relevan dalam penanganan cybercrime. Teori ini menyatakan bahwa perilaku kriminal dipelajari melalui interaksi dengan individu lain yang terlibat dalam aktivitas tersebut. Oleh karena itu, penting

[19] Ibid., halaman 3.

untuk mengidentifikasi dan mengatasi komunitas atau kelompok yang mempromosikan kejahatan siber. Intervensi dapat dilakukan dengan cara mengurangi akses pelaku ke sumber daya atau pengetahuan yang memungkinkan mereka untuk melanjutkan aktivitas kriminal, serta memberikan alternatif yang lebih positif.

2. Teori Kesempatan Kriminal (*Routine Activities Theory*)

   Teori Kesempatan Kriminal (*Routine Activities Theory*), yang dikembangkan oleh Lawrence Cohen dan Marcus Felson, berfokus pada bagaimana peluang kejahatan muncul dari rutinitas sehari-hari dan situasi. Teori ini menekankan bahwa kejahatan terjadi ketika ada peluang yang terbuka dan adanya pelaku yang berniat jahat serta kurangnya pengawasan. Untuk menangani cybercrime berdasarkan teori ini, langkah-langkah pencegahan seperti memperketat kontrol akses ke sistem, meningkatkan pengawasan jaringan, dan mengurangi celah keamanan yang dapat dimanfaatkan oleh pelaku kejahatan merupakan strategi yang efektif.

3. Teori Strain (*Strain Theory*)

   Teori Strain (*Strain Theory*), yang diperkenalkan oleh Robert Merton, menganggap bahwa tekanan dan ketidakpuasan terhadap pencapaian tujuan sosial dapat memicu perilaku kriminal. Dalam konteks cybercrime, ini bisa diterjemahkan sebagai frustrasi atau tekanan yang dirasakan oleh individu yang mungkin merasa terpinggirkan atau tidak memiliki akses yang sama dengan orang lain. Untuk mengatasi cybercrime dari sudut pandang ini, penting untuk

menangani faktor-faktor sosial dan ekonomi yang dapat berkontribusi pada perilaku tersebut, seperti meningkatkan kesempatan pendidikan dan ekonomi yang setara.

4. Teori Kontrol Sosial (Social Control Theory)

   Teori Kontrol Sosial (Social Control Theory) dari Walter Reckless juga relevan, yang membahas bagaimana kekuatan kontrol sosial baik dari luar maupun dalam individu dapat mempengaruhi perilaku kriminal. Dalam konteks cybercrime, kontrol sosial bisa berupa kebijakan perusahaan yang ketat, pengawasan komunitas online, serta penguatan nilai-nilai etika dalam penggunaan teknologi. Dengan memperkuat kontrol sosial baik di tingkat individu maupun institusi, dapat mengurangi kemungkinan terjadinya kejahatan siber.[20]

2. Mengubah Tampilan Situs Web

Berbagai banyak kejahatan yang sering terjadi, diantaranya kejahatan dunia maya atau yang biasa disebut dengan cyber crime dimana seseorang melakukan aktivitas kejahatan dengan komputer atau jaringan komputer. Sementara menurut *Organation Of European Comunity Development* (OECD) cybercrime adalah semua bentuk akses ilegal terhadap suatu transmisi data, artinya semua bentuk kegiatan yang tidak sah dalam suatu sistem komputer termasuk dalam suatu tindak kejahatan. Dengan

[20] Deri Malian, (2024),"Penanganan dan Tantangan Cybercrime Di Era Digital Perspektif Kriminologi", Innovative: Journal Of Social Science Research, halaman 6.

maraknya perkembangan teknologi saat ini, kejahatan digital juga semakin marak dilakukan oleh oknum yang tidak bertanggungjawab. Diantaranya seperti defacing.[21]

Deface adalah kegiatan hacking yang mengubah tampilan sebuah website. Sedangkan cara yang digunakan bisa bermacam-macam seperti SQL Injection, mencari password, dan cara lainnya. Deface adalah Aktifitas yang mengotori, "menodai", merubah inti dari isi halaman suatu website dengan tulisan, gambar, ataupun link yang membuat suatu link menjadi melenceng dari perintah yang kita buat. Sedangkan pengertian dari web deface adalah melakukan perubahan pada halaman web depan pada situs-situs tertentu, dilakukan oleh para hacker atau cracker untuk mengganggu informasi yang dimunculkan pada halaman situs yang dimaksud. Pengertian mudahnya, web deface adalah menambahkan gambar, tulisan ke suatu web milik orang lain tanpa sepengetahuan adminnya.

Defacing adalah merupakan bagian dari kegiatan hacking web atau program application, yang menfokuskan target operasi pada perubahan tampilan dan konfigurasi fisik dari web atau program aplikasi tanpa melalui source code program tersebut. Sedangkan deface itu sendiri adalah hasil akhir dari kegiatan cracking. Tekniknya adalah dengan membaca source codenya, terus ngganti image dan editing html tag.[22]

Istilah website defacement/defacing mengacu pada serangan yang mengubah tampilan situs web atau halaman web dengan menyerang ketersediaan dan integritas

---

[21] Dewi Nur, Diana, Nur Muhammad Amin, Moh. Zeinudin, (2023) "Analisis Kriminologis Defacing Dalam Bentuk Cyber Crime", Jurnal Sumenep, Vol. 5, No.6, halaman 214.

[22] Tanti Siti Nurjanah, Entik Insanudin, (2016) "Hack Database Website Menggunakan Python Sqlmap Pada Windows", Jurnal:Uin Sunan Gunung Djadi Bandung, halaman 3.

yang dilakukan tanpa adanya otorisasi akses terhadap website tersebut sehingga, peretasan/hacking dan website defacement/defacing seringkali dikaitkan. Tindakan peretasan ini tidak hanya diakukan pada akun media sosial seseorang namun juga dapat dilakukan pada situs web, baik milik pribadi maupun milik pemerintah. Orang yang melakukan deface/defacing/website defacement disebut dengan defacer.

Berdasarkan dampak yang dapat terjadi pada halaman situs yang terkena serangan terkait maka, deface dapat dibagi menjadi dua jenis yaitu:

1. *Full of page*

   Melakukan deface terhadap satu beranda/halaman penuh tampilan depan alias file index/file lainnya akan diubah secara utuh merupakan pengertian full of page dari jenis tindak pidana defacing. Jenis ini dilakukan oleh seorang defacer yang biasanya harus memiliki akses secara 'langsung' terhadap box (mesin) atau defacer tersebut berusaha memiliki keuntungan/privileged terhadap box (mesin) terkait, termasuk root account ataupun hal lain yang dapat melancarkan aksi defacer untuk secara interaktif mengendalikan index file dan lainnya secara menyeluruh. Defacer dapat melaksanakan aksinya dengan memanfaatkan kekurangan pada services yang ada di mesin yang kemudian melakukan akses ilegal ke mesin.

2. Sebagian atau hanya menambahi

   Jenis defacing kedua yang dapat dilakukan oleh defacer yaitu 'sebagian/hanya menambahi". Yaitu, defacer melakukan defacing/mendeface suatu website/situs tidak secara menyeluruh/penuh. Defacer biasanya melakukan

dengan adanya penampilan beberapa gambar, kata maupun script yang tidak pantas dan mengganggu.[23]

Ada 2 tahapan dari terjadinya defacing/ tindak pengubahan tampilan website/ website defacement, yaitu:

1. Tahap pertama, dilakukan dengan cara menerobos sistem orang lain atau kedalam web server,
2. tahap kedua adalah mengganti halaman website (web page).

Sehingga, peretasan/hacking dan website defacement/defacing dari hacking. Kegiatan menyusup yang dilakukan kepada sistem komputer maupun jaringan yang pada umumnya bertujuan untuk merusak ataupun menyalahgunakan sistem yang ada.Hacking memiliki definisi sebagai kegiatan penyusupan ke dalam sebuah sistem komputer maupun jaringan bertujuan untuk merusak ataupun menyalahgunakan sistem yang ada. Oleh karena itu menurut penulis, tanpa melakukan peretasan/hacking maka defacer tidak dapat mengubah tampilan indeks file suatu website baik itu secara menyeluruh maupun sebagian saja.[24]

Beberapa cara yang dapat digunakan untuk mengamankan sistem informasi berbasis internet adalah:

1. Mengatur akses (*access control*)Salah satu cara yang umum digunakan untuk mengamankan informasi adalah dengan mengatur akses ke informasi melalui

[23] Novita, (2023) "Tinjauan Yuridis Tindak Pidana Defacing Pada Kasus Pengubahan Tampilan Website Milik KPU Kabuoaten Jember", Skripsi: Universitas Hasanuddin Makasar, halaman 30.
[24] Ibid., halaman 31.

mekanisme authentication dan access control. Implementasi dari mekanisme ini antara lain dengan menggunakan password. Di sistem UNIX dan Windows NT, untuk masuk dan menggunakan sistem komputer, pemakai harus melalui proses *authentication* dengan menuliskan userid (*user identification*) dan password.

2. Menutup service yang tidak digunakan Dalam sebuah sistem seringkali perangkat keras dan perangkat lunak diberikan beberapa service yang dijalankan sebagai default, seperti pada sistem UNIX yang sering dipasang dari vendornya adalah *finger, telnet, ftp, smtp, pop, echo*, dan sebagainya.untuk mengamankan sistem servis maka server yang tidak diperlukan dimatikan.
3. Memasang proteksi Untuk lebih meningkatkan keamanan sistem informasi, proteksi dapat ditambahkan. Proteksi ini dapat berubah filter lebih khusus firewall. Filter dapat digunakan untuk memfilter e-mail, informasi, akses atau bahkan dalam level packet.Ada program filter internet yang bernama Zeeksafe. Program ini bisa memblokir situs-situs yang tidak diinginkan selama pengguna surfing di internet.Selain itu ada juga We-Blocker Yang menentukan parameter apa saja yang akan membatasi akses ke website yang dianggap tidak layak dilihat.
4. FirewallFirewall merupakan sebuah perangkat yang diletakkan antara internet dengan jaringan internet. Informasi yang keluar atau masuk harus melalui firewall ini.Tujuan utama dari firewall adalah untuk menjaga (*prevent*) agar akses ke dalam maupun ke luar dari orang yang tidak berwenang (*unauthorized access)* tidak dapat dilakukan.Firewall bekerja dengan mengamati paket

Internet Protocol(IP) yang melewatinya. Detail dari konfigurasi bergantung kepada masing-masing firewall, Firewall dapat berupa sebuah perangkat keras yang sudah dilengkapi dengan perangkat lunak tertentu sehingga pemakai (administrator) tinggal melakukan konfigurasi dan firewall tersebut. Firewall Juga dapat berupa perangkat lunak yang ditambahkan pada sebuah server (baik UNIX maupun Windows NT) yang dikonfigurasikan menjadi firewall. Firewall biasanya melakukan 2 (dua) fungsi, yaitu fungsi Internet Protocol(IP) filtering dan fungsi proxy.

5. Pemantau adanya serangan Sistem pemantauan (monitoring system) digunakan untuk mengetahui adanya tamu tidak diundang (intruder) atau adanya serangan (attack). Nama lain dari sistem ini adalah Intruder Detection System(IDS). Sistem ini dapat memberi tahu administrator melalui e-mail maupun melalui mekanisme lain seperti pager. Ada beberapa cara untuk memantau adanya intruder, baik yang sifatnya aktif maupun pasif. Intruder Detection System (IDS) cara yang pasif misalnya dengan memonitor log file. Beberapa contoh dari Intruder Detection System (IDS), antara lain:
    a) Autobuse, mendeteksi probing dengan memonitor log file
    b) Courtneydan portsentry, mendeteksi probing (*port scanning*)dengan memonitor packet yang lalu lalang. Portsentry Bahkan dapat memasukkan Internet Protocol(IP) penyerang dalam filter tcp wrapper.
    c) Shadowdari SANS.
    d) Snort, mendeteksi pola (pattern) pada paket yang lewat dan

mengirimkan alert jika pola tersebut terdeteksi. Pola-pola atau rules disimpan dalam berkas yang disebut library yang dapat dikonfigurasi sesuai dengan kebutuhan.

Password dapat saja menjadi sistem pengaman yang baik asalkan tidak membiarkan password itu digunakan untuk jangka waktu yang tidak terlalu lama dan selalu dalam pengawasan. Penggunaan password yang sama dan terlalu lama sangat berbahaya, karena dalam keadaan administrator lemah, cracker dapat masuk ke sistem dan mengeksploitasinya. Kelemahan dari pengelolaan password seperti ini terutama terjadi pada hari-hari dimana administrator libur atau pada hari-hari dimana jam kerja diliburkan.

Perlindungan pemilik website dalam upaya pencegahan dan penanggulangan kriminalisasi cybercrime di Indonesia secara yuridis sudah dilindungi oleh hukum akan tetapi belum begitu tegas diatur oleh salah satu perundang-undangan yang secara khusus mengatur tentang kriminalisasi cybercrime ini. Hal inilah yang menjadi salah satu penyebab semakin maraknya kriminalisasi cybercrime yang sangat merugikan pemilik website.[25]

Pengaturan tindak pidana defacing dirumuskan dalam Undang-Undang Nomor 11 Tahun 2008 sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik. Akan tetapi, sejarah penormaan pidana terhadap kejahatan defacing juga pernah dilakukan dengan menggunakan

[25] Dewi Nur, Diana, Nur Muhammad Amin, Moh. Zeinudin*, Op.cit*., halaman 216.

ketentuan mengenai kejahatan terhadap barang atau benda dalam Pasal 406 ayat (1) Kitab Undang-Undang Hukum Pidana (KUHP). Penggunaan pasal tersebut merupakan upaya untuk mengisi kekosongan hukum terhadap kejahatan defacing di masa lalu yakni dengan penafsiran obyek benda sebagai benda tidak berwujud termasuk elektronika dan komputer. Selain itu, tindak pidana defacing juga pernah dikenakan pidana sesuai rumusan Pasal 22 Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi. Namun ketentuan defacing dalam undang-undang tersebut kurang komprehensif dalam pengaturannya karena hanya mencakup unsur illegal access.[26]

Dalam UU ITE mengenai perbuatan defacing termasuk ke dalam perbuatan yang dilarang yang apabila dilihat dari tahap awal melakukan defacing yaitu melakukan Illegal access, bahwa illegal access telah diatur pada Undang-Undang Nomor 11 Tahun 2008 sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 Pasal 30 ayat (1), (2) dan (3), yang berbunyi :

1. Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau Sistem Elektronik milik orang lain dengan cara apapun.
2. Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau Sistem Elektronik dengan cara apa pun dengan tujuan untuk memperoleh informasi Elektronik dan/atau Dokumen Elektronik.
3. Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau Sistem Elektronik dengan cara apa pun dengan melanggar,

[26] Ibid., halaman 217.

menerobos, melampaui, atau menjebol sistem pengaman.[27]

Undang-Undang Nomor 11 Tahun 2008 sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 Pasal 30 ayat (1), (2) dan (3), pada intinya berbicara mengenai illegal access yang apabila pasal tersebut dikaitkan dengan defacing menggunakan metode penafsiran ekstensif, maka diperlukan suatu tindakan untuk menerobos sistem orang lain tanpa izin dengan hacking defacing.[28]

[27] Penjelasan Umum atas Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 Tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik

[28] Novita, Op.cit.,halaman 37.

BAB III

PEMBAHASAN

A. Faktor-Faktor Yang Menjadi Penyebab Terjadinya Tindakan Mengubah Tampilan Situs Web Tanpa Izin

Tindak kejahatan dan perbuatan tercela merupakan perilaku yang melanggar hukum dan norma sosial, dan masyarakat tidak menerimanya. Tindak kejahatan sering kali disebabkan oleh berbagai banyak faktor. Faktor pemicu terjadinya tindak kejahatan adalah faktor biologis yang terdiri dari faktor ekonomi (tidak adanya lapangan pekerjaan), faktor mental atau fisik, dan faktor pribadi, faktor sosial, dan masih banyak faktor lainnya sebagai pemicu berbagai macam jenis tindak kejahatan. Tindak kejahatan dan perbuatan tercela merupakan perbuatan yang melanggar hukum dan melanggar norma sosial, dan masyarakat menentangnya. Tindakan pidana atau tindakan kriminal memiliki dampak yang sangat merugikan dalam kehidupan sosial di masyarakat Indonesia, sehingga dapat menimbulkan kecemasan, ketakutan, kecemasan, dan kepanikan di kalangan masyarakat Indonesia.

Dengan meningkatnya kasus tindak kriminal dan revolusi dunia, khususnya peningkatan tindak kriminal di internet sangat tambah kekhawatiran, penegakan hukum merupakan inti utama dalam melawan tindakan kriminal di internet, sehingga penegakan hukum harus bekerja keras.[29]

[29] Fiqqih Anugrah, Tantimin, (2022)," Pencurian Data Pribadi Di Internet Dalam Perspektif Kriminologi", Junal Komunikasi Hukum, Vol.8, No.1, halaman 428.

Tindak pidana kejahatan pada teknologi informasi dapat diklasifikasikan sebagai *white crime* dikarenakan para pelaku kriminal di dunia maya merupakan seseorang yang memahami pemakaian aplikasi internet, atau mahir pada bagian tersebut. Karena tindak kriminal ini kerap dilakukan dengan cara transnasional atau secara melewati pemisah antar negara, tindak kriminal dunia maya ini disertai dengan dua kriteria kriminal, diantara lain white crime dan transnational crime. Terdapat beberapa kasus tindak kriminal di internet (cyber crime) yang kerap beraksi di kalangan masyarakat di Indonesia yakni penipuan, judi online, penyebaran berita hoax, cracking, hingga pencurian data pribadi melalui internet. Bidang keamanan komputer terus berkembang pesat karena teknologi informasi semakin mempengaruhi pola kehidupan masyarakat di Indonesia seperti bekerja, berkomunikasi, berbelanja, dan lain-lainnya. Dengan perkembangan tersebut, ancaman terhadap keamanan komputer semakin meningkat, baik ancaman fisik maupun non fisik seperti kerentanan sistem operasi, serangan jaringan, dan virus. Aspek keamanan mutlak diperlukan dalam pengaturan sistem jaringan berbasis internet. Sistem tanpa sistem keamanan yang baik seperti mengundang pencuri ke rumah kita dan membiarkan mereka mengambil semua yang kita miliki. Saat membangun sebuah sistem, berbagai kerentanan sering ditemukan di dalam sistem. Namun, itu tidak dianggap sebagai kerentanan keamanan (hole), sehingga dianggap kecil. Celah keamanan sekecil itu tidak kita ketahui dan digunakan oleh para pelaku kriminal untuk melakukan aksi kejahatan.[30]

[30] Ibid., halaman 429.

Sutherland mengajukan 9 proposisi tentang proses terjadinya tingkah laku jahat, yaitu sebagaimana dikemukakan Bartollas berikut.

1. Tingkah laku jahat, sebagaimana perilaku lainnya, dipelajari dari orang lain. Perilaku jahat bukan perilaku yang diwariskan.
2. Tingkah laku jahat dipelajari dalam hubungan interaksi dengan orang lain melalui proses komunikasi, baik langsung maupun tidak langsung.
3. Bagian terpenting dari mempelajari tingkah laku jahat terjadi dalam kelompok intim, lebih efektif dibandingkan dengan komunikasi bentuk lainnya, misalnya lewat film atau surat kabar;
4. Mempelajari tingkah laku jahat termasuk di dalamnya teknik melakukan kejahatan dan motivasi / dorongan atau alasan pembenar termasuk sikap-sikap;
5. Arah dari motif dan dorongan tertentu dipelajari melalui definisi-definisi dari peraturan perundang- undangan. Dalam masyarakat kadang- kadang anak berhubungan dengan orang-orang yang melihat apa yang diatur dalam peraturan perundang-undangan/hukum sebagai sesuatu yang perlu diperhatikan dan dipatuhi, tetapi kadang seorang anak juga dapat berhubungan dengan orang- orang yang melihat aturan hukum sebagai sesuatu yang memberi peluang untuk melakukan kejahatan).
6. (Seseorang menjadi delinkuen, karena ekses dari pola- pola pikir yang lebih melihat aturan hukum sebagai pemberi peluang dilakukannya kejahatan

daripada yang melihat hukum sebagai sesuatu yang harus diperhatikan dan dipatuhi).

7. Asosiasi diferensial ini bervariasi tergantung dari frekuensi, jangka waktu, prioritas dan intensitasnya. Jadi dampak negatif yang ditimbulkan oleh kelompok (peers groups) tergantung pada frekuensi, seberapa lama, pengalaman, dan intensitas dalam bergaul).
8. Proses mempelajari tingkah laku jahat melalui pergaulan dengan pola kejahatan dan anti-kejahatan melibatkan semua mekanisme yang berlaku dalam setiap proses belajar. Jadi mempelajari tingkah laku jahat tidak terbatas pada upaya meniru tingkah laku).
9. Sekalipun tingkah laku jahat merupakan pencertfiinan dari kebutuhan-kebutuhan umum dan nilai-nilai, tetapi tingkah laku jahat tersebut tidak dapat dijelaskan melalui kebutuhan umum dan nilai-nilai, karena tingkah laku yang tidak jahat pun merupakan pencerminan dari kebutuhan-kebutuhan umum dan nilai nilai yang sama. Jadi motif seseorang yang terlibat kenakalan berbeda dengan perilaku pada umumnya, karena dasar pemahamannya juga berbeda).[31]

Tindak kejahatan di bidang teknologi informasi sering dikategorikan sebagai *white crime* karena pelakunya memiliki pemahaman dan keahlian dalam menggunakan

[31] Hardianto Djanggih, Nurul Qamar, (2018),"Peneapan Teori-Teori Kriminologi dalam Penanggulangan Kejahatan Siber (Cyber Crime)", Jurnal Pandecta, Vol.13, No.1, halaman 16.

aplikasi internet atau bidang terkait. Karena kejahatan ini sering melintasi batas negara dan dilakukan secara transnasional, kejahatan dunia maya ini dapat digolongkan sebagai dua jenis kejahatan, yaitu white crime dan transnational crime.

Dalam sudut pandang kriminologi, ada beberapa faktor dan alasan yang menyebabkan kasus cybercrime terjadi. Dari segi alasan, kejahatan ini biasanya dapat dibagi menjadi dua kategori, yaitu:

1. Motif intelektual kriminal terjadi saat seseorang melakukan kejahatan semata-mata untuk kepuasan pribadi dan untuk menunjukkan kemampuannya dalam merancang dan menerapkan teknologi informasi. Motif ini umumnya dilakukan oleh individu.
2. Motif ekonomi, politik, dan kriminalitas merujuk pada alasan di balik suatu tindak kriminal yang dilakukan dengan tujuan memperoleh keuntungan pribadi atau kelompok yang dapat merugikan pihak lain baik secara ekonomi maupun politis. Kriminalitas dengan motif ini, bertujuan untuk menciptakan dampak besar dan sering kali dilakukan oleh perusahaan atau korporasi.[32]

Faktor-faktor yang menyebabkan terjadinya tindak pidana dunia maya (cybercrime) yang merupakan induk dari tindak pidana peretasan (hacking). Faktor faktor tersebut adalah :

[32] Muhammad Fadli, Dijan Widijowati, Dwi Andayani, (2024),"Pencurian Data Pribadi di Dunia Maya (Phising Cyber Crime) Yang ditinjau dalam Perspektif Kriminologi", Jurnal Ekonomi, Koperasi & Kewirausahaan, Vol.14. No.12, halaman 6.

1. Akses internet yang tidak terbatas, dengan menggunakan internet, setiap orang diberikan kenyamanan dalam mengakses segala sesuatu tanpa ada batasannya. Dengan kenyamanan itulah yang merupakan faktor utama bagi sebagian orang untuk melakukan tindak pidana dunia maya (cyber crime) dengan mudahnya.
2. Kelalaian pengguna komputer. Dimana orang-orang menggunakan fasilitas internet selalu memasukkan semua data penting ke dalam internet, sehingga memberikan kemudahan bagi sebagian orang untuk melakukan tindak pidana tersebut.
3. Mudah dilakukan dengan risiko keamanan yang kecil dan tidak diperlukan peralatan yang super modern. Walaupun tindak pidana dunia maya mudah untuk dilakukan tetapi akan sangat sulit untuk melacaknya, sehingga hal ini yang mendorong para pelaku tindak pidana untuk terus melakukan hal ini.
4. Pera pelaku merupakan orang yang pada umumnya cerdas, mempunyai rasa ingin tahu yang besar dan fanatik akan teknologi komputer. Pengetahuan pelaku tindak pidana peretasan tentang cara kerja sebuah komputer jauh di atas rata-rata orang pada umumnya. e) Sistem keamanan jaringan yang lemah. f) Kurangnya perhatian masyarakat.

Faktor-faktor penyebab terjadinya tindak pidana peretasan (hacking) terbagi menjadi 2 faktor yaitu :

1. Faktor-faktor internal penyebab terjadinya peretasan (hackig)
    a. Tindak pidana peretasan (hacking) dilakukan oleh pelaku karena didorong motif dendam, iseng, dan atau hanya untuk memenuhi kepuasan pribadi.
    b. Tindak pidana peretasan (hacking) dilakukan atas dasar kepentingan pribadi baik yang bersifat materi maupun non materi.
    c. Tindak pidana peretasan (hacking) tidak melakukan tindakan pengrusakan apapun tetapi hanya melakukan eksplorasi dan penetrasi terhadap sebuah sistem operasi dan kode komputer pengaman lainnya.
2. Faktor-faktor eksternal penyebab terjadinya peretasan (hacking):
    a. Kurangnya pengetahuan penegakn hukum di negara Republik Indonesia dalam mengatasi masalah peretasan (hacking).
    b. Sistem keamanan jaringan yang belum bisa mencegah terjadinya tindak pidana peretasan (hacking).
    c. Belum adanya badan-badan khusus bentukan pemerintah yang bisa memberikan bantuan terhadap terjadinya tindak pidana peretasan (hacking).[33]

Untuk mengetahui terjadinya tindak kejahatan kita harus mengetahui mengapa seseorang itu dapat melakukan kejahatan serta apa saja faktor pendorong seseorang

[33] Henny Saida Flora, (2025),"Faktor Penyebab dan Penanggulangan Terjadinya Peretasan Whatsapp", Jurnal Profile Hukum, Vol.3, No.1, halaman 5.

melakukan kejahatan. Beberapa pendapat para ahli mengenai faktor penyebab tidak bertanggung jawab untuk melakukan terjadinya kejahatan:

Faktor-faktor penyebab terjadinya kejahatan dalam bidang perbankan yang menggunakan fasilitas komputer (komputer sebagai sarana kejahatan) dalam Penelitian Aman Nursusila di Bagian Serse Ekonomi Polda Jawa Timur dan Polwil Malang, menyimpulkan bahwa factor penyebabnya adalah karena mencoba kemampuan di bidang teknologi internet (66,6%), dan karena alasan ekonomi (33,3%).

Perkembangan jaman melahirkan kejahatan baru di bidang teknologi informasi, faktor yang mempengaruhi diantaranya:

Faktor Segi teknis, tidak bisa dipungkiri bahwa kemajuan teknologi (teknologi informasi) berdampak negatif bagi perkembangan Berhasilnya teknologi masyarakat. tersebut menghilangkan batas wilayah negara menjadikan dunia ini menjadi begitu sempit keterhubungan antara jaringan yang satu dengan jaringan yang lain memudahkan bagi si pelaku kejahatan untuk melakukan aksinya. Kemudian, tidak meratanya penyebaran teknologi menjadikan yang satu lebih kuat daripada yang lain. Kelemahan tersebut dimanfaatkan oleh mereka yang tidak bertanggung jawab untuk melakukan kejahatan:

a. Faktor sosio ekonomi, cybercrime merupakan produk ekonomi. Isu global yang kemudian dihubungkan dengan kejahatan tersebut adalah keamanan jaringan (security network). Keamanan jaringan merupakan isu global yang digulirkan

berbarengan dengan internet. Sebagai komoditi ekonomi, banyak negara yang tentunya sangat membutuhkan perangkat keamanan jaringan. Cybercrime berada dalam skenario besar dari kegiatan ekonomi dunia.

b. Faktor Perkembangan Teknologi Perkembangan, teknologi khususnya teknologi informasi dan komunikasi selain memberikan dampak positif juga memberikan dampak negatif terhadap masyarakat diseluruh dunia karena selain dapat mengubah perilaku dan peradapan manusia serta menyebabkan perubahan soaial, perkembangan teknologi informasi yang meningkat membuat dunia menjadi tanpa batas sehingga banyak muncul kejahatan baru yang memanfaat internet sebagai modus operandi.
c. Faktor Lemahnya Sistem Pengawasan, lemahnya sistem pengawasan dari bank penerbit. Karena dengan kemajunya teknologi informasi mengharuskan lembaga perbankkan untuk bisa terus bergerak dan mengikuti perkembangan kejahatan yang dilakukan di dunia maya dengan tujuan untuk memudahkan kebutuhan nasabah, sehingga aparat pengawas bank harus terus meningkatkan kemampuannya terus menerus secara supaya berkesinambungan dapat mendeteksi potensi kejahatan carding itu sendiri.
d. Faktor Pengguna Kecerobohan Internet, Para para pengguna internet harus mulai sadar akan adanya cybercrime yang mengintai kita setiap saat dengan cara meretas atau membuat situs-situs internet berbahaya. Para pengguna harus mulai sadar akan pentingnya sistem keamanan jaringan agar komputer mereka

agar bisa terlindung dari bahaya cybercrime khususnya kejahatan carding yang sangat merugikan.[34]

Pelaku tindakan *deface web* seringkali mengincar website yang memiliki celah dan kelemahan dalam keamanannya, peretas akan menggunakan berbagai teknik penyerangan untuk melakukan eksploitasi kelemahan ataupun celah dalah keamanan website target sehingga peretas dapat memiliki akses kedalam server target untuk melakukan berbagai macam tindakan kejahatan seperti deface website untuk berbagai macam hal seperti menunjukkan kelemahan keamanan, melakukan propaganda politik dan agama, menjual produk, untuk kesenangan pribadi,dll.[35] Adapun Faktor terjadinya defacing, sebagai berikut:

1. Faktor Internal
    a. Kesalahan Konfigurasi

        Apabila tidak di konfigurasikan dengan baik malah akan menjadi boomerang bagi sistem itu sendiri. Bisa jadi sesuai dengan istilah "pagar makan tanaman". Perlu adanya ketelitian dan pengecekan ulang.

    b. Kelalaian admin

        Apabila Konfigurasi telah sesuai, maka factor "man behind the gun" yang akan berbicara banyak; sehingga factor internal kedua adalah manusia yang menggelola server tersebut.

---

[34] M.Nanda Setiawan, Mariana Safitri, Lidya Lestari, (2022),"Kejahatan Carding Sebagai Bentuk Cyber Crime Dalam Hukum Pidana Indonesia", Datin Law Jurnal, Vol.3, No.2, halaman 170

[35] Brian Budi Aji, (2023),"Tindakan Kejahatan Cyber Crime Dalam Bentuk Deface Website", Jurnal Cyber Security dan Forensik Digital, Vol.6, No.1, halaman 27.

Adapun jenis kelalaian yang dapat terjadi adalah:

1) Install File dan Folder

   Webmaster atau admin biasanya lalai dalam menghapus file yang digunakan untuk menginstallasi web model CMS.

   Contoh: Folder/install dan file install.php pada phpnuke, postnuke, phpbb.

2) File Konfigurasi dan permission

   Webmaster atau admin lupa mengatur permisi pada file-file konfigurasi yang penting, yang menyangkut administrasi dan konfigurasi file, khususnya file-file yang mencatat password, baik password database dsb.

   Contoh: File config.txt, config.php, config.inc.

3) Run of date

   Terlalu lama pen-update-an suatu web atau tidak secara terus-terusan mengupdate webnya khususnya portal yang dibundel dalam CMS, serta juga packet-packet yang terinstalasi di mesin baik itu web server sendiri, database server dan sebagainya yang bisa menjadi pintu masuk bagi defacer.

4) Run of service

   Kesalahan konfigurasi tehadap services/layanan yang diberikan khususnya terlalu banyak menjalankan layanan yang tidak diperlukan pada setiap server.

2. Factor Eksternal

   a. *Sofware vulnerabilities*

      Software vulnerabilities disini adalah kelemahan, atau kesalahan yang dimiliki oleh *software*/ program yang dipakai baik secara sengaja atau tidak sengaja. Khususnya *software-software open source*/ atau yang berlisensi GPL (*General Public License*), maka tidaklah aneh apabila dalam hitungan hari, atau malah jam dapat diketahui kelemahan suatu *software* banyak situs yang membahas dan melaporkan *vulnerabilities* suatu *software* baik itu situs resmi *software* tersebut atau situs situs keamanan, info ini bisa menjadi senjata ampuh bagi para *defacer* atau bahkan bisa menjadi perisai ampuh bagi *webmaster* atau *admin.*

   b. Sistem *vulnerabilities*

      Sistem operasi dari *server* khususnya *kernel* yang dikembangkan oleh pengembang khususnya *Kernel* (http://Kernel.org) sehingga bukannya tidak mungkin kebocoran ini diperbaiki ahli. kasus seperti ini cukup jarang, umumnya cara yang ditempuh bisa dilakukan secara local/ *lokal exploit* kecuali eksploitasi pada DCOM RPC yang berakibat kesalahan itu bisa di eksploitasi secara *remote* dan berbahaya sekali bagi mesin dikarenakan akan memberikan akses *administrator.*

   c. *Run of control*

      Suatu kesulitan untuk melakukan kontrol terhadap beberapa metode serangan terbentuk oleh *administrator,* hal itu bisa dikarenakan penggunaan

beberapa fasilitas atau metode serangan yang cukup relatif sulit untuk dihindari.

serangan serangan ini sangat umum diketahui di antaranya:

1) *Brute Forcing*

   Brute force attack adalah jenis serangan yang dilakukan dengan melakukan berbagai bentuk kombinasi karakter yang akan di cobakan sebagai *password* detail soal BFA (*Brute Force Attack).* Metode ini mungkin yang paling Kekal, alias sudah lama tetapi tetap dipakai dikarenakan kelebihannya yaitu tidak perlu mengetahui sistem enkripsi, atau metoda pengamanan khususnya untuk *login.* tetapi memiliki berbagai keterbatasan tersendiri, baik dalam hal kecepatan khususnya.

   Contoh: penggunaan *brutus* sebagai program yang cukup ampuh untuk membuat *password* baik ftp. http, smtp, dsb.

2) *Dictionary attack*

   Metode ini menggunakan kamus kata yang sering digunakan, walau tetap memiliki prinsip yang sama dengan *Brute forcing.* target serangan ini adalah *password*, atau bisa dikatakan *attack* terhadap *authentication*.

3) *DOS attack*

Daniel of servis adalah aktivitas penghambat kerja sebuah layanan servis atau mematikannya sehingga *user* yang berkepentingan tidak dapat menggunakan layanan tersebut.

4) *Sniffing*

Sniffing adalah kegiatan menyadap atau menginfeksi paket data menggunakan *sniffer software* atau *hardware* di internet. biasa digunakan Ettercap, erhereal.[36]

B. Bentuk-Bentuk Kejahatan Terhadap Tindakan Mengubah Tampilan Situs Web Tanpa Izin

Teknologi informasi dan komunikasi telah dimanfaatkan dalam kehidupan sosial masyarakat, dan telah memasuki berbagai faktor kehidupan baik sektor pemerintahan, bisnis, perbankan, pendidikan, kesehatan, dan kehidupan pribadi. Manfaat teknologi informasi dan komunikasi selain memberikan dampak positif juga disadari memberi peluang untuk dijadikan sarana melakukan kejahatan baru (cyber crime). sehingga dapat dikatakan bahwa teknologi informasi dan komunikasi bagaikan pedang bermata dua, dimana selain memberikan kontribusi positif kesejahteraan, bagi kemajuan, peningkatan peradaban manusia, juga menjadi sarana potensial dan sarana efektif untuk melakukan perbuatan melawan hukum.

[36] M.Ade Chairuddin Najib, (2018),"Sanksi Terhadap Tindak Pidana Defacing dalam Undang-undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik dengan Perspektif Hukum Islam", Skripsi Universitas Islam Raden Fatah Palembang, halaman 69.

Cyber crime dapat diartikan sebagai kegiatan illegal dengan perantara komputer yang dapat dilakukan melalui jaringan elektronik global. Pada jaringan kmputer seperti internet, masalah kriminalitas menjadi semakin kompleks karena ruang lingkupnya yang luas. Kriminalitas dalam internet atau cyber crime pada dasarnya adalah suatu tindak pidana yang berkaitan degnan cyber space,baik yang menyerang fasilitas umum di dalam cyber space ataupun kepemilikan pribadi.[37]

Berbagai banyak kejahatan yang sering terjadi, diantaranya kejahatan dunia maya atau yang biasa disebut dengan cyber crime dimana seseorang melakukan aktivitas kejahatan dengan komputer atau jaringan komputer. Sementara menurut Organation Of European Comunity Development (OECD) cybercrime adalah semua bentuk akses ilegal terhadap suatu transmisi data, artinya semua bentuk kegiatan yang tidak sah dalam suatu sistem komputer termasuk dalam suatu tindak kejahatan. Dengan maraknya perkembangan teknologi saat ini, kejahatan digital juga semakin marak dilakukan oleh oknum yang tidak bertanggungjawab. Diantaranya seperti defacing.[38]

Istilah website defacement/defacing mengacu pada serangan yang mengubah tampilan situs web atau halaman web dengan menyerang ketersediaan dan integritas yang dilakukan tanpa adanya otorisasi akses terhadap website tersebut sehingga, peretasan/hacking dan website defacement/defacing seringkali dikaitkan. Tindakan peretasan ini tidak hanya diakukan pada akun media sosial seseorang namun juga dapat

[37] Henny Saida Flora,(2025),"Faktor Penyebab dan Penanggulangan Terjadinya Pretasan Whatsapp", Jurnal Profile Hukum, Vol.3, No.1, halaman 2.

[38] Dewi nur Diana, Nur Muhammad Amin, Moh. Zeinudin, (2023),"Analisis Kriminologis Defacing Dalam Bentuk Cyber Crime", Jurnal Sumenep, Vol.5, No.6, halaman 214.

dilakukan pada situs web, baik milik pribadi maupun milik pemerintah. Orang yang melakukan deface/defacing/website defacement disebut dengan defacer.

Lebih singkatnya bahwa defacing dapat didefinisikan sebagai suatu tindakan penyusupan ke dalam suatu situs atau website yang kemudian mengubah tampilan halaman dari situs dengan tujuan tertentu. Website defacement/defacing dapat mengakibatkan terjadinya dampak kerugian materil dan formil baik secara langsung maupun tidak langsung. Website defacement/defacing dapat dilakukan untuk berbagai alasan, yang sebagian besar akan dianggap sebatas alasan ekspresif yang dilatarbelakangi oleh emosional langsung dibandingkan dengan alasan adanya manfaat ekonomi bagi pelaku/penyerang.[39]

Berdasarkan dampak yang dapat terjadi pada halaman situs yang terkena serangan terkait maka, *deface* dapat dibagi menjadi dua jenis yaitu:

1. Full of page

   Artinya Mendeface satu halaman Penuh tampilan depan alias File Index atau file lainnya yang akan diubah secara utuh, artinya untuk melakukan ini biasanya seorang ‘defacer’ umumnya harus berhubungan secara langsung dengan box (mesin) atau usaha mendapatkan Priveleged terhadap mesin, baik itu root account atau sebagainya yang memungkinkan defacer dapat secara Interaktif mengendalikan File indek dan lainnya secara utuh. Umumnya dengan

[39] Novita, (2023),”Tinjauan Yuridis Tindak Pidana Defacing Pada Kasus Pengubahan Tampilan Website Milik KPU Kabupaten Jember”, Skripsi Universitas Hassanuddin Makassar, halaman 28.

memanfaatkan kelemahan pada services-services yang berjalan di mesin, sehingga dapat melakukan pengaksesan ke mesin.

2. Sebagian atau hanya menambahi

   Artinya, defacer mendeface suatu situs tidak secara penuh, bisa hanya dengan menampilkan beberapa kata gambar atau penambahan script-script yang menganggu, hal ini umumnya hanya akan memperlihatkan tampilan filr yang di deface menjadi kacau dan umumnya cukup mengganggu, defacer biasanya mencari celah baik dari kelemahan scripting yang digunakan dengan XSS injection, bisa dengan SQL atau database injection dan juga beberapa vulnerabilities yang seringkali ditemukan pada situs-situs yang dibangun dengan menggunakan CMS (Content Manajemen System).[40]

Beberapa teknik yang umum digunakan dalam deface situs web, seperti serangan injeksi SQL, Remote File Inclusio (RFI), Local File Inclusion (LFI), dan Cross-Site Scripting (XSS). Mereka menjelaskan bagaimana teknik ini bekerja dan bagaimana para pelaku bisa mendapatkan keuntungan darinya.[41]

SQL injection merupakan teknik yang disukai oleh para hacker karena selama ini masih banyak website yang kurang memperhatikan celah keamanan pada sistemnya yang dapat dimanfaatkan oleh pengguna yang tidak bertanggung jawab. Injeksi SQL dapat terjadi karena penyerang yang menguasai teknik query SQL dapat mem-bypass

[40] M.Ade Chairuddin Najib, Op.cit., halaman 64.
[41] Dewi Nur Diana, Nur Muhammad Amin, Moh. Zeinuddin, Op.cit., halaman 214.

lubang keamanan di SQL pada lapisan basis data aplikasi. Kerentanan terjadi karena input formulir pengguna tidak difilter dengan benar untuk karakter meta saat menulis menggunakan input formulir. Jadi, selama ini sql injector masih menjadi tool favorit para attacker untuk melakukan penyerangan pada website. Apalagi sekarang hacking melalui internet sudah tidak sesulit dulu lagi. Sekali lagi, serangan injeksi SQL sering terjadi karena kelalaian programmer (pengembang aplikasi) yang tidak mengimplementasikan pembatas filter untuk karakter metadata (&, ;, ', ', \, " , |, *, ?, ~, < ;, >, ^ , (,) , [,], {, }, $, \n, \r) digunakan dalam sintaks SQL aplikasi input formulir, sehingga penyerang dapat memasukkan wildcard ini menggunakan kombinasi kueri skrip sehingga tindakan liar dapat dilakukan dengan mengautentikasi penetrasi Jika aplikasi web tidak menerapkan filter pada input formulir, penyerang dapat meluncurkan serangan dengan memasukkan nama pengguna dengan menambahkan '#', misalnya 'rudz#' Hal ini menyebabkan karakter selanjutnya tidak diperlakukan sebagai kode SQL, sehingga username "rudz" tidak perlu memasukkan password untuk masuk ke system.

Teknik lain yang umum digunakan adalah inklusi file jarak jauh (RFI) dan inklusi file lokal (LFI). RFI melibatkan penggunaan lubang keamanan dalam aplikasi web untuk mengimpor dan mengeksekusi kode berbahaya dari sumber eksternal. Padahal, LFI melibatkan pemanggilan file lokal yang tidak dapat diakses oleh pengguna biasa.

Inklusi file jarak jauh adalah lubang keamanan memungkinkan penyerang untuk memasukkan file berbahaya dari luar server dan menjalankannya, file ini biasanya mengandung kesalahan kode berbahaya atau kode yang dapat digunakan untuk mengontrol komputer atau server korban. Jarak ini tampaknya salah satu karena konfigurasi di server salah dan pengkodean tidak divalidasi dan benar. Dampak Kerentanan seperti itu dapat diakses oleh penyerang file sensitif bahkan dapat memanipulasi file secara langsung file, tampilkan database, ubah izin dan itu kasus terburuk mengambil kendali server.

Inklusi file lokal adalah lubang keamanan memungkinkan penyerang untuk membaca atau melihat file di server termasuk file sensitif. LFI biasanya muncul karena kesalahan coding, salah satunya disebabkan oleh fungsi seperti fungsi include() itu tidak diautesntikasi dan difilter dengan benar. Fungsi include() adalah fungsi dari bahasa pemrograman PHP masukkan fungsi atau string sesuatu seperti file dalam halaman di situs web. Kapan fungsi ini tidak diautentikasi dengan benar, serangan LFI bisa berjalan di halaman tertentu. Dampak serangan LFI adalah kemampuan untuk membaca file sensitif yang ada di server, misalnya file sensitif di server Linux. Contohnya adalah file /etc/passwd, dalam file ini berisi informasi sensitif seperti nama pengguna, kata sandi terenkripsi, ID pengguna, ID grup, dll. Informasi ini tidak boleh diketahui oleh siapa pun yang tidak memiliki izin atau akses ke server.

Selain itu, serangan Cross-Site Scripting (XSS) juga biasa digunakan untuk mengubah situs web. Dalam serangan ini, pelaku menyisipkan kode skrip berbahaya

ke dalam halaman web, yang kemudian dijalankan oleh browser pengguna. Ini memungkinkan penulis mencuri informasi sensitif, mengarahkan pengguna ke halaman palsu, atau mengubah tampilan dan nuansa situs.[42]

Terdapat beberapa bentuk kejahatan yang berhubungan dengan penggunaan teknologi informasi yang berbasis utama komputer dan jaringan telekomunikasi:

1. *Unauthorized Access to Computer System and Service*, yaitu kejahatan yang dilakukan dengan memasuki atau menyusup ke dalam suatu sistem jaringan komputer secara tidak sah (tanpa izin ataupun sepengetahuan dari pemilik sistem jaringan komputer yang dimasukinya).
2. *Illegal Contents*, yakni kejahatan dengan memasukkan data atau informasi ke internet tentang sesuatu hal yang tidak benar, tidak etis, dan dapat dianggap melanggar hukum atau mengganggu ketertiban umum. Sebagai contoh, pemuatan suatu berita bohong atau fitnah yang akan menghancurkan martabat atau harga diri pihak lain.
3. *Cyber Espionage*, yakni kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer (computer network system) pihak sasaran.
4. *Cyber Sabotage and Extortion*, merupakan kejahatan yang dilakukan dengan membuat gangguan, perusakan dan peghancuran terhadap suatu data,

[42] Brian Budi Aji, (2023),” Tindakan Kejahatan Cyber Crime Dalam Bentuk Deface Website”, Jurnal Cyber Security dan Forensik Digital, Vol.6, No.1, halaman 26.

program komputer atau sistem jaringan komputer yang tersambung dengan internet. Biasanya kejahatan ini dilakukan dengan menyusupkan suatu logic bomb, 22 virus komputer ataupun suatu program tertentu, sehingga data, program komputer atau sistem jaringan komputer tidak dapat dijalankan sebagiamana mestinya. Dalam beberapa kasus terjadi pekaku kejahatan menawarkan diri kepada korban untuk memperbaikinya dengan bayaran tertentu.

5. *Offense against Intellectual Property*, yakni kejahatan yang umumnya ditujukan untuk melanggar hak atas kekayaan intelektual yang dimiliki pihak lain di internet. Sebagai contoh, peniruan tampilan pada web page suatu situs milik orang lain secara ilegal, penyiaran suatu informasi di internet yang ternyata merupakan rahasia dagang orang lain, dan sebagainya.
6. *Infringements of Privacy*. Kejahatan ini biasanya ditujukan terhadap keterangan pribadi seseorang yang tersimpan pada formulir data pribadi yang tersimpan secara computerized yang apabila diketahui oleh orang lain maka dapat merugikan korban secara materil maupun immateril, seperti nomor kartu kredit dan nomor PIN ATM.[43]

Di dalam cybercrime terdapat istilah hactivism, yaitu aktivitas yang dilakukan oleh hacker. Aktivitas kejahatan tersebut dilakukan dengan dua tahap: pertama-tama

[43] Ahmad Muyasir, (2015),"Kejahatan Defecting: Studi Perbandingan antara Undang-Undang ITE dan Hukum Pidana Islam", Jurnal Al-Mazahib, Vol.3, No.1, halaman 148.

pelaku melakukan hacking (pembobolan sistem computer)26 dan setelah itu pelaku kemudian melakukan activism. Adapun hactivism sendiri berbeda dengan cyberterrorism sekalipun keduanya ada unsur kesamaannya (sama-sama dilakukan dengan terlebih dahulu melakukan hacking), tetapi berbeda dalam tujuan dan akibatnya. Jika cyberterrorism bertujuan, antara lain, menimbulkan ketakutan, maka hactivism sama sekali tidak menimbulkan ketakutan dan hanya bermaksud mencemooh korban. Jika dilihat dari sisi akibat yang ditimbulkan, maka cyberterrorism dapat mengakibatkan kerugian yang dahsyat kepada masyarakat, seperti merusak sistem informasi bank sentral, merusak jaringan listrik, dan merusak jaringan badan pengawas pasar modal, sedangkan hactivism paling jauh hanya mengubah tampilan situs atau defacing dan tidak menimbulkan korban jiwa atau kerusakan terhadap infrastruktur dan property masyarakat.

Hactivism itu sendiri memiliki beragam bentuk. Alexandra Whitney Samuel sebagaimana dikutip oleh Sutan Remi Syahdeini menyebutkan sembilan bentuk kejahatan komputer (electronic mischief), yaitu:

1. Site Defacement/defacing / pengubahan tampilan situs,
2. Site Direct / pembelokan situs,
3. Denial of serice attack / serangan-serangan DOS,
4. Information theft / pencurian informasi,
5. Information theft and distribution / pencurian informasi dan pendistribusian informasi curian tersebut,
6. Virtual sit-ins / pendudukan situs,

7. Site parody / parody situs,
8. Virtual sabotage / sabotase virtual,
9. Software development / pengembangan perangkat lunak).

Dari paparan di atas tampak jelas bahwa terdapat berbagai macam hactivism, dan defacing hanyalah salah satu bentuk dari hactivism itu. Defacing merupakan aktivitas modification; dalam arti tindakan melakukan perubahan terhadap data atau informasi atau konten yang mengalir dalam sebuah infrastruktur teknologi informasi tanpa sepengetahuan yang mengirimkan atau menerimanya.[44]

C. Upaya Penanggulangan Hukum Pidana Terhadap Tindakan Mengubah Tampilan Situs Web Tanpa Izin

Upaya penanggulangan kejahatan telah dan terus dilakukan oleh semua pihak, baik pemerintah maupun masyarakat pada umumnya. Berbagai program dan kegiatan telah dilaksanakan sambil terus mencari cara tepat dan efektif untuk mengatasi masalah tersebut. Dalam hukum pidana Sanksi hukuman dari pemidanaan itu sendiri bisa dilihat pada Pasal 10 KUHPidana yaitu ditetapkannya pidana mati, denda, kurungan ataupun penjara dan ini merupakan pidana pokok. Di samping itu, hukuman pidana lainnya dapat diterapkan, seperti pencabutan hak-hak tertentu, pengumuman putusan hakim, dan penyitaan barang-barang tertentu.[45]

---

[44] Ibid., halaman 150.

[45] Putri Dharmayani Siregar, Harisman, (2024),"Tindak Pidana Kekerasan Fisik Dalam Kekerasan Rumah Tangga", Jurnal Ilmu Hukum Vol.8, No.3, halaman 635.

Dalam hubungan ini E.H. Sutherland dan Cressesy mengemukakan bahwa dalam crime prevention dalam pelaksanaannya ada dua buah metode yang dipakai untuk mengurangi frekuensi kejahatan yaitu:

1. Metode untuk mengurangi penanggulangan dari kejahatan, merupakan suatu cara yang ditujukan kepada pengurangan jumlah dilakukan secara konseptual.
2. Metode untuk mencegah kejahatan pertama kali, suatu cara yang ditujukan kepada upaya untuk mencegah terjadinya kejahatan yang pertama kali, yang akan dilakukan oleh seseorang dalam metode ini dikenal sebagai metode preventif.

Berdasarkan uraian diatas dapat dilihat bahwa upaya penanggulangan kejahatan mencakup aktivitas preventif sekaligus berupaya memperbaiki prilaku seseorang dinyatakan telah bersalah (terpidana) di Lembaga Pemasyarakatan atau dengan kata lain, upaya kejahatan dapat dilakukan secara pre-emptif, preventif dan represif. Menurut A.S. Alam, penanggulangan kejahatan terdiri atas tiga bagian pokok, yaitu:

1. Upaya *Pre-emtif*

   Upaya pre-emtif (moral) adalah upaya awal yang dilakukan oleh pihak kepolisian untuk mencegah terjadinya kejahatan. Dalam upaya ini yang lebih ditekankan adalah menanamkan nilai/norma dalam diri seseorang.

2. Upaya *Preventif*

   Upaya penanggulangan kejahatan secara *preventif* (pencegahan) dilakukan untuk mencegah timbulnya kejahatan pertama kali. Mencegah kejahatan lebih baik daripada mencoba mendidik penjahat menjadi lebih baik kembali,

demikian semboyan dalam kriminologi, yaitu usaha-usaha memperbaiki penjahat (narapidana) yang perlu diperhatikan dan diarahkan agar tidak terjadi lagi kejahatan ulang.

3. Upaya *Represif*

   Upaya *represif* adalah suatu upaya penanggulangan kejahatan secara konsepsional yang ditempuh setelah terjadinya kejahatan. Penanggulangan dengan upaya represif dimaksudkan untuk menindak para pelaku kejahatan sesuai dengan perbuatannya serta memperbaiki kembali agar mereka sadar bahwa perbuatan yang dilakukannya merupakan perbuatan yang melanggar hukum dan merugikan masyarakat, sehingga tidak akan mengulanginya dan orang lain juga tidak akan melakukannya mengingat sanksi yang akan ditanggungnya sangat berat. [46]

Berbagai banyak kejahatan yang sering terjadi, diantaranya kejahatan dunia maya atau yang biasa disebut dengan *cyber crime* dimana seseorang melakukan aktivitas kejahatan dengan komputer atau jaringan komputer. Sementara menurut Organation *Of European Comunity Development* (OECD) *cybercrime* adalah semua bentuk akses ilegal terhadap suatu transmisi data, artinya semua bentuk kegiatan yang tidak sah dalam suatu sistem komputer termasuk dalam suatu tindak kejahatan. Dengan

[46] Varhan Herman, (2019),"Tinjauan Kriminologis Terhadap Kejahatan Penipuan Yang Dilakukan Melalui Media Elektronik", Skripsi Universitas Hasanuddin Makassar, halaman 26.

maraknya perkembangan teknologi saat ini, kejahatan digital juga semakin marak dilakukan oleh oknum yang tidak bertanggungjawab. Diantaranya seperti *defacing*.

Secara terminologi, istilah *defacing* merupakan bentuk kata benda dari kata kerja *deface* yang artinya merusakkan, mencemarkan, menggoresi, menghapus. Akan tetapi penggunaan istilah ini di dalam dunia hukum *cyber crime* diidentikkan sebagai sebuah kegiatan mengubah tampilan halaman utama atau halaman lain dari suatu website yang bersangkutan baik itu didalam folder maupun file.

Pemahaman yang mendalam tentang teknik *deface* website sangat penting dalam upaya pencegahan serangan dan menjaga keamanan sistem informasi. Dengan mengetahui cara kerjanya dan kerentanan yang digunakan, perlindungan yang lebih efektif dapat diterapkan untuk mengurangi risiko degradasi situs.[47]

Menanggapi masalah kejahatan Indonesia telah memiliki peraturan perundang-Undangan yang cukup untuk menindak tindak kejahatan Perundangan dunia maya (Defacing) ini. Secara umum, Perundangan dunia maya (Defacing) dapat saja di interpretasikan terhadap berbagai delik yang diatur dalam hukum pidana umum di Indonesia, yaitu yang temuat dalam kitab Undang-Undang Hukum Pidana (KUHP), Pasal-Pasal KUHP yang relevan dalam mengatur delik Perundangan dunia maya (defacing) ini adalah yang tercantum dalam Bab XXVII tentang penghancuran atau perusakan barang, Khusunya Pasal 406 ayat (1) dan (2).

[47] Dewi nur Diana, Nur Muhammad Amin, Moh. Zeinudin, (2023),"Analisis Kriminologis Defacing Dalam Bentuk Cyber Crime", Jurnal Sumenep, Vol.5, No.6, halaman 214.

Pada dasarnya, KUHP memang dibentuk jauh sebelum perkembangan teknologi dunia maya dicetuskan. Maka, dalam rangka mengakomodasi pengaturan mengenai dunia maya dan segala hal yang berkaitan dengannya, dibentuklah Undang-Undang Nomor 11 Tahun 2008 tentang Infomasi dan Transaksi Elektronik yang kini telah di revisi menjadi Undang-Undang Nomor19 Tahun 2016. Dalam undang-undang ini, terdapat pasal-pasal yang dikira lebih sesuai untuk menjerat para pelaku Perundangan dunia maya (defacing).[48]

UURI Nomor 11 Tahun 2008 merupakan undang-undang pertama dalam ranah Teknologi Informasi dan Traksaksi Elektronik yang menjadi produk legislasi yang sangat dibutuhkan dan telah menjadi pionir yang meletakkan dasar pengaturan dalam pemanfaatan Teknologi Informasi dan Transaksi Elektronik. Di dalam UU ITE mengenai perbuatan defacing termasuk ke dalam perbuatan yang dilarang yang apabila dilihat dari tahap awal melakukan defacing yaitu melakukan Illegal access, bahwa illegal access telah diatur pada Pasal 30 ayat (1), (2) dan (3), yang berbunyi:

1) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau Sistem Elektronik milik orang lain dengan cara apapun.
2) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau Sistem Elektronik dengan cara apa pun dengan tujuan untuk memperoleh informasi Elektronik dan/atau Dokumen Elektronik.

[48] M.Ade Chairuddin Najib, (2018),” Sanksi Terhadap Tindak Pidana Defacing Dalam Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik Dengan Perspektif Hukum Islam”, Skripsi Universitas Islam Negeri Raden Fatah Palembang, halaman 75.ive

3) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau Sistem Elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengaman.

Pasal 30 dari ayat (1), ayat (2) dan ayat (3) pada intinya berbicara mengenai *illegal access* yang apabila pasal tersebut dikaitkan dengan *defacing* menggunakan metode penafsiran ekstensif, maka diperlukan suatu tindakan untuk menerobos sistem orang lain tanpa izin atau yang biasa disebut dengan hacking sebelum melakukan *defacing. Defacing* diatur pula pada Pasal 32 ayat (1) yang berbunyi:

"*Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun mengubah, menambahkan, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang Lain atau milik publik*".[49]

Berdasarkan uraian di atas, defacing merupakan perbuatan/tindak pidana yang diatur dalam Kitab Undang-Undang Hukum Pidana (KUHP) dan juga diatur dalam Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 Tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (UU ITE).

Defacing yang tergolong ke dalam tindak pidana perusakan dan penghancuran secara umum (lex generalis) diatur dalam KUHP, tetapi secara khusus (lex spesialis) defacing yang merupakan kejahatan di dunia maya dengan menggunakan sarana

[49] Novita, (2023),"Tinjauan Yuridis Tindak Pidana Defacing Pada Kasus Pengubahan Tampilan Website Milik KPU Kabupaten Jember", Skripsi Universitas Hasanuddin Makassar, halaman 37.

teknologi informasi dalam melancarkan aksinya ini diatur dalam Undang-Undang Nomor 11 Tahun 2008 jo. Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE).[50]

Berdasarkan teori kriminologi, penanganan *cybercrime* dapat dilihat melalui beberapa perspektif yang membantu memahami dan mengatasi kejahatan siber secara efektif. Salah satu teori utama yang relevan adalah:

1. Teori Keseimbangan Sosial (*Social Control Theory*).

Teori ini menekankan bahwa hubungan sosial yang kuat dan komitmen terhadap norma-norma sosial berfungsi sebagai penghalang terhadap perilaku kriminal. Dalam konteks *cybercrime*, pendekatan ini mendorong upaya untuk membangun kesadaran dan kepatuhan terhadap norma-norma keamanan siber melalui edukasi dan pelatihan, baik di kalangan individu maupun organisasi. Dengan memperkuat ikatan sosial yang mendukung perilaku aman di dunia maya, risiko terjadinya cybercrime dapat dikurangi.

2. Teori Pembelajaran Sosial (*Social Learning Theory*).

Teori ini dikemukakan oleh Albert Bandura, juga relevan dalam penanganan cybercrime. Teori ini menyatakan bahwa perilaku kriminal dipelajari melalui interaksi dengan individu lain yang terlibat dalam aktivitas tersebut. Oleh karena itu, penting untuk mengidentifikasi dan mengatasi komunitas atau kelompok yang mempromosikan kejahatan siber. Intervensi dapat dilakukan dengan cara mengurangi

[50] Ibid.,halaman 39.

akses pelaku ke sumber daya atau pengetahuan yang memungkinkan mereka untuk melanjutkan aktivitas kriminal, serta memberikan alternatif yang lebih positif .

3. Teori Kesempatan Kriminal (*Routine Activities Theory*).

Teori ini dikembangkan oleh Lawrence Cohen dan Marcus Felson, berfokus pada bagaimana peluang kejahatan muncul dari rutinitas sehari-hari dan situasi. Teori ini menekankan bahwa kejahatan terjadi ketika ada peluang yang terbuka dan adanya pelaku yang berniat jahat serta kurangnya pengawasan. Untuk menangani *cybercrime* berdasarkan teori ini, langkah-langkah pencegahan seperti memperketat kontrol akses ke sistem, meningkatkan pengawasan jaringan, dan mengurangi celah keamanan yang dapat dimanfaatkan oleh pelaku kejahatan merupakan strategi yang efektif.

4. Teori Strain (*Strain Theory*).

Teori ini diperkenalkan oleh Robert Merton, menganggap bahwa tekanan dan ketidakpuasan terhadap pencapaian tujuan sosial dapat memicu perilaku kriminal. Dalam konteks *cybercrime*, ini bisa diterjemahkan sebagai frustrasi atau tekanan yang dirasakan oleh individu yang mungkin merasa terpinggirkan atau tidak memiliki akses yang sama dengan orang lain. Untuk mengatasi *cybercrime* dari sudut pandang ini, penting untuk menangani faktor-faktor sosial dan ekonomi yang dapat berkontribusi pada perilaku tersebut, seperti meningkatkan kesempatan pendidikan dan ekonomi yang setara.

5. Teori Kontrol Sosial (*Social Control Theory*)

Teori ini diperkenalkan Walter Reckless juga relevan, yang membahas bagaimana kekuatan kontrol sosial baik dari luar maupun dalam individu dapat

mempengaruhi perilaku kriminal. Dalam konteks *cybercrime*, kontrol sosial bisa berupa kebijakan perusahaan yang ketat, pengawasan komunitas online, serta penguatan nilai-nilai etika dalam penggunaan teknologi. Dengan memperkuat kontrol sosial baik di tingkat individu maupun institusi, dapat mengurangi kemungkinan terjadinya kejahatan siber.

Secara keseluruhan, pendekatan berbasis teori kriminologi dalam penanganan *cybercrime* melibatkan pemahaman tentang penyebab dan motivasi di balik perilaku kriminal, serta penerapan strategi yang sesuai untuk mencegah, mendeteksi, dan menanggulangi kejahatan siber secara efektif. Dalam hal penegakan hukum, penanganan *cybercrime* memerlukan kerjasama antara berbagai pihak, baik di tingkat domestik maupun internasional. Banyak kejahatan siber melibatkan pelaku yang beroperasi lintas batas negara, sehingga kolaborasi antara lembaga penegak hukum, badan intelijen, dan organisasi internasional sangat diperlukan.[51]

Dalam hal melakukan penegakan hukum khususnya dalam bidang kejahatan mayantara, kejahatan ini memiliki jangkauan yang sangat luas tanpa mengenal batas wilayah territorial suatu negara karena kejahatan ini bersifat transnasional. Tipe kejahatan yang tak mengela batas ini mengharuskan yurisdiksi suatu negara terlibat langsung di dalamnya karena sangat jauh dari jangkauan suatu negara. Jika tanpa melakukan kerja sama antara negara dalam melakukan pemberantasan serta penegakan

[51] Deri Malian, (2024),"Penanganan Dan Tantangan Cybercrime di Era Perspektif Kriminologi", Journal Of Social Science Research, Vol.4, No.6, halaman 2024.

hukum yang sebagaimana mestinya, kejahatan yang bersifat transnasional ini akan menimbulkan masalahnya sendiri berkenaan dengan yurisdiksi.

Seringkali masalah ini menjadi sangat pelik karena kendala sebuah teritorial batas negara. Yurisdiksi dalam hal ini telah mencakup dan bertanggung jawab atas orang benda atau peristiwa hukum yang terjadi di dalamnya. Hukum internasional telah membagi beberapa prinsip yang dapat menjadi acuan dalam masalah yurisdiksi yakni prinsip territorial,prinsip nasionalitas, prinsip perlindungan serta prinsip universal.

1. Prinsip terorrial

   prinsip ini tergolong pada prinsip yang paling utama dan fundamental dalam suatu kasus yurisdiksi dimana negara berhak atas segala kasus yang terjadi dan berada dalam wilayahnya.

2. Prinsip nasionalitas

   dalam prinsip ini negara dianggap berhak untuk mengadili setiap warganegaranya terhadap segala kejahatan yang dilakukannya dimanapun warga negara tersebut berada.

3. Prinsip perlindungan

   prinsip ini lebih bersifat melindungi kepentingan vital negaranya.

4. Prinsip universal

   prinsip ini lebih bersifat umum dan sebagian dapat diterima oleh masyarakat umum, dimana dalam yurisdiksi ini setiap negara dianggap berhak atau dapat

mengadili suatu kejahatan tertentu yang dianggap membahayakan masyarakat dalam lingkup internasional.[52]

Upaya penanggulangan kejahatan sesungguhnya merupakan usaha yang terus menerus dan terus berkesinambungan. Semakin majunya peradaban manusia, sebagai implikasi dari perkembangan ilmu pengetahuan dan teknologi,muncul berbagai jenis kejahatan berdimensi baru, yang termasuk di dalamnya cyber crime. Sejalan dengan itu diperlukan upaya penanggulangan untuk menjamin ketertiban dalam masyarakat. Dalam perspektif hukum, upaya ini direalisasikan dengan hukum pidana. Hukum pidana diharapkan mampu memenuhi ketertiban masyarakat.

Dua muatan besar yang diatur dalam UU ITE ialah mengenai pengaturan tranksaksi elekronik dan mengenai tindak pidana siber. Materi UU ITE tersebut merupakan implementasi dari beberapa prinsip ketentuan internasional. Pada UU ITE dimuat tentang perbuatan yang dilarang pada Pasal 27 sampai Pasal 36. Pada pasal 42 UU ITE diatur pula mengenai ketentuan penyidikan yang berbunyi : “penyidikan sebagaimana dimaksud dalam undang-undang ini, dilakukan berdasarkan ketentuan dalam Hukum Acara Pidana dan ketentuan dalam undang undang ini”.[53]

Beberapa langkah yang disebutkan termasuk menerapkan kebijakan keamanan yang kuat, memperbarui dan memeriksa sistem secara teratur, menggunakan

---

[52] Henny Saida Flora, (2025),”Faktor Penyebab dan Penanggulangan Terjadinya Peretasan Whatsapp”, Jurnal Profile Hukum, Vol.3, No.1, halaman 7.

[53] Markus Djarawula, Novita Alfiani, Hanita Mayasari, (2023),”Tijauan Yuridis Tindak Pidana Kejahatan Teknologi Informasi (cybercrime) di Indonesia Ditinjau dari Perspektif Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik”, Jurnal Cakrawala Ilmiah, Vol.2, No.10, halaman 3804.

mekanisme autentikasi yang kuat, dan melindungi dari kerentanan yang biasa ditemukan di aplikasi web. Selain itu, juga dibahas langkah langkah pengendalian yang dapat dilakukan jika sebuah website diserang. Ini termasuk mengisolasi dan memisahkan sistem yang terpengaruh, memulihkan data dari cadangan yang aman, dan melakukan analisis forensik untuk mengidentifikasi pelaku dan sumber serangan. Secara keseluruhan, jurnal ini memberikan tinjauan komprehensif tentang teknik modifikasi situs web, tindakan pencegahan, dan kontrol yang dapat digunakan untuk melindungi situs web dari serangan jahat. Ini dapat menjadi sumber yang berguna bagi para profesional keamanan informasi dan administrator sistem yang ingin memahami dan melindungi situs web mereka dari ancaman *deface* website.

Beberapa cara yang dapat digunakan untuk mengamankan sistem informasi berbasis internet adalah:

1. Mengatur akses (*access control*) Salah satu cara yang umum digunakan untuk mengamankan informasi adalah dengan mengatur akses ke informasi melalui mekanisme authentication dan access control. Implementasi dari mekanisme ini antara lain dengan menggunakan password. Di sistem UNIX dan Windows NT, untuk masuk dan menggunakan sistem komputer, pemakai harus melalui proses *authentication* dengan menuliskan *user id (user identification)* dan *password*.
2. Menutup service yang tidak digunakan Dalam sebuah sistem seringkali perangkat keras dan perangkat lunak diberikan beberapa service yang dijalankan sebagai default, seperti pada vendornya sistem UNIX yang sering

dipasang dari adalah *finger, telnet, ftp, smtp, pop, echo*, dan sebagainya.untuk mengamankan sistem servis maka server yang tidak diperlukan dimatikan.

3. Memasang proteksi Untuk lebih meningkatkan keamanan sistem ditambahkan. Proteksi ini informasi, proteksi dapat dapat berubah filter lebih khusus firewall. Filter dapat digunakan untuk memfilter *e-mail*, informasi, akses atau bahkan dalam level packet.Ada program filter internet yang bernama *Zeeksafe*. Program ini bisa memblokir situs-situs yang tidak diinginkan selama pengguna surfing di internet.Selain itu ada juga *We-Blocker* Yang menentukan parameter apa saja yang akan membatasi akses ke website yang dianggap tidak layak dilihat.
4. *Firewall* merupakan sebuah perangkat jaringan yang diletakkan antara internet internet. Informasi yang keluar atau masuk harus dengan melalui *firewall* ini.Tujuan utama akses dari *firewall* adalah untuk menjaga (*prevent*) agar ke dalam maupun ke luar dari orang yang tidak berwenang (*unauthorized access*) tidak dapat dilakukan.*Firewall* bekerja dengan mengamati paket *Internet Protocol(IP)* yang melewatinya. Detail dari konfigurasi bergantung kepada masing-masing *firewall*, *Firewall* dapat berupa sebuah perangkat keras yang sudah dilengkapi dengan perangkat lunak tertentu sehingga pemakai (*administrator*) tinggal melakukan konfigurasi dan *firewall* tersebut. *Firewall* Juga dapat berupa perangkat lunak yang ditambahkan pada sebuah server (baik UNIX maupun Windows NT) yang dikonfigurasikan menjadi *firewall*. *Firewall*

biasanya melakukan 2 (dua) fungsi, yaitu fungsi *Internet Protocol(IP) filtering* dan fungsi *proxy*.

5. Pemantau adanya serangan Sistem pemantauan (*monitoring system*) digunakan untuk mengetahui adanya tamu tidak diundang (*intruder*) atau adanya serangan (*attack*). Nama lain dari sistem ini adalah *Intruder Detection System(IDS)*. Sistem ini dapat memberi tahu administrator melalui *e-mail* maupun melalui mekanisme lain seperti pager. Ada beberapa cara untuk memantau adanya intruder, baik yang sifatnya aktif maupun pasif. *Intruder Detection System (IDS)* cara yang pasif misalnya dengan memonitor log file. Beberapa contoh dari *Intruder Detection System (IDS),* antara lain:
   a. *Autobuse*, mendeteksi probing dengan memonitor log file.
   b. *Courtneydan portsentry*, mendeteksi *probing (port scanning*) dengan memonitor packet yang lalu lalang. Portsentry Bahkan dapat memasukkan *Internet Protocol(IP)* penyerang dalam *filter tcp wrapper.*
   c. *Shadowdari SANS*
   d. *Snort*, mendeteksi pola (*pattern*) pada paket yang lewat dan mengirimkan alert jika pola tersebut terdeteksi. Pola-pola atau rules disimpan dalam berkas yang disebut library yang dapat dikonfigurasi sesuai dengan kebutuhan.

Password dapat saja menjadi sistem pengaman yang baik asalkan tidak membiarkan *password* itu digunakan untuk jangka waktu yang tidak terlalu lama dan selalu dalam pengawasan. Penggunaan *password* yang sama dan terlalu lama sangat

berbahaya, karena dalam keadaan administrator lemah, *cracker* dapat masuk ke sistem dan mengeksploitasinya. Kelemahan dari pengelolaan *password* seperti ini terutama terjadi pada hari-hari dimana administrator libur atau pada hari-hari dimana jam kerja diliburkan.

Perlindungan pemilik website dalam upaya pencegahan dan penanggulangan kriminalisasi *cybercrime* di Indonesia secara yuridis sudah dilindungi oleh hukum akan tetapi belum begitu tegas diatur oleh salah satu perundang-undangan yang secara khusus mengatur tentang kriminalisasi *cybercrime* ini. Hal inilah yang menjadi salah satu penyebab semakin maraknya kriminalisasi *cybercrime* yang sangat merugikan pemilik website.[54]

Dari uraian di atas, dapat diketahui bahwa ada usaha yang harus dilakukan oleh pemerintah dalam menanggulangi cybercrime dengan menggunakan sarana penal, yaitu dengan membuat Undang-Undang mengenai Informasi Dan Traksaksi Elektronik No. 11 Tahun 2008 yang kemudian diubah dengan UU No. 19 Tahun 2016 dan upaya memperluas pengaturanpengaturan cyberspace dalam Kitab UndangUndang Hukum Pidana Nasional dengan memperluas beberapa pengertian yang berkaitan dengan kegiatan di *cyberspace.*

Saat ini regulasi yang dipergunakan sebagai dasar hukum atas kasus-kasus cybercrime adalah Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE). Dengan adanya UU ITE ini diharapkan dapat melindungi

[54] Dewi nur Diana, Nur Muhammad Amin, Moh. Zeinudin, Op.cit., halaman 216.

masyarakat pengguna teknologi informasi di Indonesia, hal ini penting mengingat jumlah pengguna teknologi internet yang semakin meningkat dari tahun ke tahun. Meningkatnya penggunaan internet di satu sisi memberikan banyak kemudahan bagi manusia dalam melakukan aktivitasnya, disisi lain memudahkan bagi pihak-pihak tertentu untuk melakukan suatu perbuatan tindak pidana, kemajuan teknologi ini juga mempengaruhi gaya hidup dan pola pikir manusia faktanya saat ini banyak terjadi kejahatan dengan menggunakan teknologi informasi. Fenomena cybercrime yang berkembang dengan pesat yang tidak mengenal batas teritorial ini memang harus diwaspadai karena kejahatan ini agak berbeda dengan kejahatan lain pada umumnya.

Pemanfaatan Teknologi Informasi berperan penting dalam perdagangan dan pertumbuhan perekonomian nasional untuk mewujudkan kesejahteraan masyarakat, bahwa pemerintah perlu mendukung pengembangan Teknologi Informasi melalui infrastruktur hukum dan pengaturannya sehingga pemanfaatan Teknologi Informasi dilakukan secara aman untuk mencegah penyalahgunaannya dengan memperhatikan nilainilai agama dan sosial budaya masyarakat Indonesia. Di dalam ketentuan Pasal 4 ayat (2) UU ITE disebutkan bahwa Pemerintah melindungi kepentingan umum dari segala jenis gangguan sebagai akibat penyalahgunaan Informasi Elektronik dan Transaksi Elektronik yang mengganggu ketertiban umum, sesuai dengan ketentuan Peraturan Perundangundangan.[55]

[55] Daniel F.T.Popal, (2023),"Upaya Penanggulangan Tindak Pidana Mayantara (Cybecrime)", Jurnal Fakultas Hukum Unsrat, Vol.12, No.5, halaman 9.

BAB IV

KESIMPULAN DAN SARAN

Kesimpulan

1. Pelaku tindakan deface web seringkali mengincar website yang memiliki celah dan kelemahan dalam keamanannya, peretas akan menggunakan berbagai teknik penyerangan untuk melakukan eksploitasi kelemahan ataupun celah dalam keamanan website target sehingga peretas dapat memiliki akses kedalam server target untuk melakukan berbagai macam tindakan kejahatan seperti deface website untuk berbagai macam hal seperti menunjukkan kelemahan keamanan, melakukan propaganda politik dan agama, menjual produk, untuk kesenangan pribadi,dll. Adapun Faktor terjadinya defacing adalah faktor Internal dan Eksternal.
2. hactivism, yaitu aktivitas yang dilakukan oleh hacker. Aktivitas kejahatan tersebut dilakukan dengan dua tahap: pertama-tama pelaku melakukan hacking (pembobolan sistem computer) dan setelah itu pelaku kemudian melakukan hactivism. macam hactivism, dan defacing hanyalah salah satu bentuk dari hactivism itu. Defacing merupakan aktivitas modification; dalam arti tindakan melakukan perubahan terhadap data atau informasi atau konten yang mengalir dalam sebuah infrastruktur teknologi informasi tanpa sepengetahuan yang mengirimkan atau menerimanya
3. Upaya penanggulangan kejahatan telah dan terus dilakukan oleh semua pihak, baik pemerintah maupun masyarakat pada umumnya. Berbagai program dan kegiatan telah dilaksanakan sambil terus mencari cara tepat dan efektif untuk mengatasi

masalah tersebut. upaya penanggulangan kejahatan mencakup aktivitas preventif sekaligus berupaya memperbaiki prilaku seseorang dinyatakan telah bersalah (terpidana) di Lembaga Pemasyarakatan atau dengan kata lain, upaya kejahatan dapat dilakukan secara pre-emptif, preventif dan represif.

Saran

1. Penting bagi masyarakat, khususnya generasi muda, untuk diberikan pemahaman mengenai etika dalam penggunaan teknologi informasi. Pendidikan mengenai etika digital dan konsekuensi hukum dari Tindakan meretas situs web perlu ditingkatkan di lingkungan sekolah dan kampus.
2. Aparat penegak hukum perlu dibekali dengan pengetahuan dan kemampuan teknis dalam menangani kasus kejahatan siber. Pelatihan dan kerja sama dengan Lembaga keamanan siber baik di dalam maupun luar negeri.
3. Pemilik dan Pengelola Situs Web diharapkan untuk meninkatan Sistem keamanan Situs mereka, Seperti Penggunaan firewall, Enkripsi data, dan system deteksi instrusi. Pemeliharaan rutin serta pembaharuan Perangkat lunak juga penting untuk menutup celah yang dapat dimanfaatkan oleh pihak tidak bertanggung jawab.

DAFTAR PUSTAKA

A. Buku

Barda Nawawi Arif. 2012. *Kebijakan Integral Penanggulangan Cyberporn di Indonesia*. Semarang: Lima.

Beby Suryani. 2023. *Kriminologi.* Deli Serdang: Universitas Medan Area Press.

EmiliaSusanti. *Et al.* 2018. *Hukum dan Kriminologi*. Lampung: Aura.

Faisal, et.al. 2023. *Pedo man Penulisan dan Penyelesaian Tugas Akhir Mahasiswa*. Medan: Pustaka Prima.

Ibrahim Fikma Edrisky. 2019. *Pengantar Hukum Siber*. Lampung: Sai Wawai.

Muhaimin. 2020. *Metode Penelitian Hukum*. Mataram: Mataram University Press.

Nur Solikin. 2021. *Pengantar Metodologi*. Pasuruan: CV. Penerbit Qiara Media.

Tamaulina Br.Sembiring, *et.al.* 2024. *Buku Ajar Metodologi Penelitian (Teori Praktik)*. Karawang: CV Saba Jaya Publisher.

B. Peraturan Perundang-Undangan

Undang-Undang No 11 Tahun 2008 Juncto Undang-Undang No 19 Tahun 2016 tentang Informasi dan Tranksaksi Elektronik.

Kitab Undang-Undang Hukum Pidana (KUHP).

C. Jurnal dan Karya Ilmiah

Ahmad Muyasir, ”Kejahatan Defecting: Studi Perbandingan antara Undang-Undang ITE dan Hukum Pidana Islam”, Jurnal Al-Mazahib, Vol.3, No.1, 2015.

Brian Budi Aji, “Tindakan Kejahatan Cyber Crime Dalam Bentuk Deface Website”, Cybersecurity dan Forensik Digital, Vol. 6, No. 1, 2023.

Deri Malian,"Penanganan dan Tantangan Cybercrime Di Era Digital Perspektif Kriminologi", Innovative: Journal Of Social Science Research, 2024.

Dewi Nur, Diana, Nur Muhammad Amin, Moh. Zeinudin, "Analisis Kriminologis Defacing Dalam Bentuk Cyber Crime", Jurnal Sumenep, Vol. 5, No.6, 2023.

Fathoni, S.Tisnanta, "Konstruksi Makna Izin Sebagai Instrumen Pengadilan Versus Kebijakan Kemudian Investasi Di Provinsi Lampung", Jurnal Hukum Peratun, Vol. 1,No. 1, 2018.

Fiqqih Anugrah, Tantimin, " Pencurian Data Pribadi Di Internet Dalam Perspektif Kriminologi", Junal Komunikasi Hukum, Vol.8, No.1, 2022.

Grace Yurico Bawole, "Kajian Yuridis Terhadap Perlindungan Pemilik Website Dalam Upaya Pencegahan dan Penanggulangan Kriminalisasi Cyber Crime di Indonesia", Lex Crimen Vol. 2, No. 3, 2013.

Hardianto Djanggih, Nurul Qamar, "Peneapan Teori-Teori Kriminologi dalam Penanggulangan Kejahatan Siber (Cyber Crime)", Jurnal Pandecta, Vol.13, No.1. 2018.

Harisman, "Pemanfaatan Media Sosial Online Dalam Mendukung Pembelajaran Sosiologi (Studi Kasus Kelas XI IPS)", Thesis Diploma, FIS, 2015.

Henny Saida Flora, "Faktor Penyebab dan Penanggulangan Terjadinya Peretasan Whatsapp", Jurnal Profile Hukum, Vol.3, No.1, 2025.

M.Ade Chairuddin Najib, "Sanksi Terhadap Tindak Pidana Defacing dalam Undang-undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik

dengan Perspektif Hukum Islam", Skripsi Universitas Islam Raden Fatah Palembang, 2018.

Muh. Fadli Faisal Rasyid, *et.al,* "Cybercrime Threats and Responsibities: The Utilization of Artificial Intelligence in Online Crime", Jurnal Ilmiah Mizani, Vol.11, No.1, 2024.

Muhammad Fadli, Dijan Widijowati, Dwi Andayani, " Pencurian Data Pribadi di Dunia Maya (*Phising Cybercrime*) yang ditinjau dalam Prespektif Kriminologi", Co-Value: Jurnal Ekonomi, Koperasi, Kewirausahaan, Vol. 14, No.12, 2024.

M.Nanda Setiawan, Mariana Safitri, Lidya Lestari, "Kejahatan Carding Sebagai Bentuk Cyber Crime Dalam Hukum Pidana Indonesia", Datin Law Jurnal, Vol.3, No.2, 2022.

Novita, "Tinjauan Yuridis Tindak Pidana Defacing Pada Kasus Pengubahan Tampilan Website Milik KPU Kabuoaten Jember", Skripsi: Universitas Hasanuddin Makasar, 2023.

Putri Dharmayani Siregar, Harisman,"Tindak Pidana Kekerasan Fisik Dalam Kekerasan Rumah Tangga", Jurnal Ilmu Hukum Vol.8, No.3, 2024.

Tanti Siti Nurjanah, Entik Insanudin, "Hack Database Website Menggunakan Python Sqlmap Pada Windows", Jurnal:Uin Sunan Gunung Djadi Bandung, 2016.

Varhan Herman, "Tinjauan Kriminologis Terhadap Kejahatan Penipuan Yang Dilakukan Melalui Media Elektronik", Skripsi Universitas Hasanuddin Makassar, halaman, 2019.