

**TINJAUAN YURIDIS PERTANGGUNGJAWABAN TINDAK PIDANA PERETASAN
PADA SITUS WEB DI INTERNET (*DEFACING*) BERDASARKAN UNDANG-
UNDANG NOMOR 1 TAHUN 2024 TENTANG INFORMASI DAN TRANSAKSI
ELEKTRONIK**

Fariddudin Imam Hastomo, Lindri Purbowati
Program Studi Strata Satu (S-1) Ilmu Hukum Fakultas Hukum
Universitas Dirgantara Marsekal Suryadarma
faridimam2003@gmail.com, lindri@unsurya.ac.id

Abstract

As technology advances, so does the proliferation of crimes with negative impacts. Crimes stemming from the growth and advancement of information technology include internet-related crimes, also known as cybercrime. One such crime is website defacing or hacking. Defacing is carried out with the aim of damaging or changing the appearance of a website's homepage. This action is often carried out to tarnish the reputation of an organization or individual, exploit weaknesses in security systems, or convey political or ideological messages. This study aims to identify perpetrator accountability and law enforcement regarding website hacking in the context of digital crime based on Law Number 1 of 2024 concerning Information and Electronic Transactions. The research method in writing this scientific journal uses a normative juridical research method which is carried out by reviewing library materials such as theories, legal principles, books, or previous research journals that already exist, as well as laws and regulations and legal doctrines related to writing research. The results of the study show that the Electronic Information and Transactions Law has regulated appropriately regarding the crime of defacing and law enforcement in Indonesia regarding cybercrime, especially defacing, often experiences obstacles, especially in the arrest of suspects and confiscation of evidence.

Keywords: *Accountability, Hacking, Defacing*

Abstrak

Semakin berkembangnya teknologi, semakin berkembang pula kejahatan yang membawa dampak negatif. Kejahatan yang disebabkan dari pertumbuhan dan majunya suatu teknologi informasi ialah kejahatan yang berhubungan dengan internet atau bisa juga dikenal dengan istilah cybercrime. Salah satunya ialah defacing

Article History

Received: Agustus 2025
Reviewed: Agustus 2025
Published: Agustus 2025

**Copyright : Author
Publish by : CAUSA**



This work is licensed under a [Creative Commons Attribution-NonCommercial 4.0 International License](https://creativecommons.org/licenses/by-nc/4.0/).

atau peretasan Website. Defacing dilakukan dengan tujuan merusak atau mengubah tampilan beranda suatu situs web. Tindakan ini sering dilakukan untuk mencoreng nama baik suatu organisasi atau individu, mengeksploitasi kelemahan dalam sistem keamanan, atau menyampaikan pesan politik atau ideologi. Penelitian ini bertujuan untuk mengidentifikasi pertanggungjawaban pelaku dan penegakan hukum mengenai peretasan situs web dalam konteks kejahatan digital Berdasarkan Undang-Undang Nomor 1 Tahun 2024 Tentang Informasi dan Transaksi Elektronik. Metode penelitian pada penulisan jurnal ilmiah ini menggunakan metode penelitian penelitian yuridis normatif yang dilakukan dengan cara menelaah bahan-bahan kepustakaan seperti teori, asas hukum, buku, atau jurnal penelitian terdahulu yang telah ada, serta peraturan perundang-undangan maupun doktrin-doktrin hukum yang berkaitan dengan penulisan penelitian. Hasil penelitian menunjukkan bahwa Undang-Undang Informasi dan Transaksi Elektronik sudah mengatur dengan tepat terkait tindak pidana defacing dan penegakan hukum di Indonesia terkait cybercrime khususnya defacing seringkali mengalami hambatan terutama dalam penangkapan tersangka dan penyitaan barang bukti

Kata Kunci : Pertanggungjawaban, Peretasan, Defacing

PENDAHULUAN

Bidang segi teknologi informasi adalah suatu bidang di kehidupan bermasyarakat yang memiliki pertumbuhan serta evolusi yang bisa dibilang sangat cepat. Globalisasi yang sudah menjadi pendukung dari lahirnya era perkembangan teknologi informasi. Peristiwa cepatnya dari pertumbuhan teknologi tersebut telah meluas keseluruh dunia. Tidak terjadi di negara yang maju saja, namun di negara yang berkembang pun telah memacu pertumbuhan teknologi informasi pada warganya tersendiri. Oleh karena itu teknologi informasi mendapatkan kondisi yang penting bagi majunya sebuah bangsa. Maka dari itu pembentuk undang-

undang yang mengatur mengenai bidang teknologi informasi perlu mengantisipasi perkembangan tersebut dengan cara membentuk undang-undang yang dapat mengakomodasi perkembangan yang akan terjadi.¹

Semakin berkembangnya teknologi tersebut maka semakin berkembang pula kejahatan yang membawa dampak negatif. Kejahatan yang disebabkan dari pertumbuhan dan majunya suatu teknologi informasi ialah kejahatan yang berhubungan dengan internet atau bisa juga dikenal dengan istilah *cybercrime*. Secara umumnya yang dimaksud dengan *cybercrime* atau kejahatan didunia komputer ialah usaha untuk masuk serta menggunakan fasilitas dan alat komputer atau jaringan komputer tanpa seizin serta melawan hukum dengan atau tanpa menyebabkan perubahan serta kerusakan pada fasilitas-fasilitas komputer yang dimasuki atau digunakan tersebut.²

Salah satu media yang sangat berguna dalam perkembangan teknologi komunikasi saat ini adalah situs web. Situs web berfungsi sebagai saluran untuk mengakses informasi dan iklan di dunia daring, termasuk profil pribadi, akademis, dan bisnis, serta berita pendidikan dan bisnis, dan informasi terkini. Situs web memudahkan kita untuk berbagi dan mendapatkan informasi yang kita butuhkan. Situs web memiliki berbagai tujuan, termasuk media promosi, pemasaran, informasi, instruksi, dan komunikasi.³

Salah satu keuntungan dari situs web atau *website* adalah fakta bahwa keberadaan internet telah menciptakan paradigma baru dalam kehidupan. Seperti yang disebutkan sebelumnya, berfungsi sebagai saluran untuk mengakses informasi dan iklan di dunia daring, termasuk profil pribadi, akademis, dan bisnis, serta berita pendidikan dan bisnis, dan informasi terkini. Kehidupan berubah dari yang asli (nyata) ke yang baru, yaitu yang maya atau tidak asli (*virtual*). Keduanya biasa

¹ Suhariyanto Budi, *Tindak Pidana Teknologi Informasi (CyberCrime) Urgensi Pengaturan dan Celah Hukumnya* (Jakarta: Rajawali Pers, 2014), hlm 1.

² Dikdik M. Arief Mansur dan Elisatris Gultom, *Cyber Law Aspek Hukum Teknologi Informasi* (Bandung: Refika Aditama, 2009), hlm 8.

³ Darmawan Deni dan Hendra Deden Permana, *Desain dan Pemograman Website* (Bandung: Remaja Rosdakarya, 2013), hlm 5.

dihubungkan dengan internet serta ruang cakupan di dunia maya (*cyberspace*).⁴ Setelah hadirnya *cyberspace* memberikan peluang akan terjadinya pidana atau dikenal dengan nama *cybercrime* (kejahatan di dunia maya), jenis *cybercrime* salah satunya ialah *defacing* atau peretasan *Website*.⁵

Cyberspace yaitu suatu area imajiner tanpa batas yang dimana mengakses dan mendapatkan informasi tentang berbagai hal yang kemudian seiring perkembangan teknologi yaitu melahirkan istilah baru yang dikenal sebagai *Cybercrime*⁶, *cybercrime* saat ini merujuk pada suatu tindakan kejahatan yang berhubungan dengan dunia maya (*cyberspace*) dan tindakan kejahatan yang menggunakan komputer. Ada ahli yang menyamakan antara tindak kejahatan *cyber* (*cybercrime*) dengan tindak kejahatan komputer, dan ada ahli yang membedakan di antara keduanya. Meskipun belum ada kesepakatan mengenai definisi kejahatan Teknologi Informasi, namun ada kesamaan pengertian universal mengenai kejahatan komputer⁷

Defacing merupakan tindakan yang dilakukan oleh seorang *hacker* atau peretas dengan tujuan merusak atau mengubah tampilan beranda suatu situs web. Tindakan ini sering dilakukan untuk mencoreng nama baik suatu organisasi atau individu, mengeksploitasi kelemahan dalam sistem keamanan, atau menyampaikan pesan politik atau ideologi. Kejahatan dunia maya berupa perusakan situs web memiliki konsekuensi serius, baik bagi pemilik situs web maupun bagi pengguna yang mengandalkan informasi atau layanan yang ada di dalamnya.⁸

Perihal Peretasan *Website* diatur dalam beberapa Undang-Undang. Dimulai dari Undang-Undang Nomor 11 Tahun 2008.⁹ Dan dirubah

⁴ Abdul Wahid, Mohammad Labib, *Kejahatan Mayantara (Cyber Crime)*, (Bandung: Refika Aditama, 2010), hlm 103.

⁵ Dikdik M. Arief Mansur dan Elisatris Gultom, Op. Cit., hlm 4.

⁶ Situmeang, Sahat Maruli T. "*Cyber law*." (Bandung: CV Cakra, 2020), hlm 9.

⁷ Dikdik M. Arief Mansur dan Elisatris Gultom, Op. Cit., hlm 7.

⁸ Brian Budi Aji, *Tindakan Kejahatan Cyber Crime Dalam Bentuk Deface Website: Cyber Security Dan Forensik Digital*, *Jurnal Universitas Islam Negeri Sunan Kalijaga* (Vol. 6 No. 1 2023) hlm 25

⁹ Indonesia, Undang-Undang Informasi dan Transaksi Elektronik, Undang-Undang Nomor. 11 Tahun 2008.

menjadi Undang-Undang Nomor 1 Tahun 2024.¹⁰ Tentang Informasi dan Transaksi Elektronik yang disahkan pemerintah di tanggal 2 Januari 2024, lalu *Defacing* juga bersinggungan dengan Undang-Undang lainnya seperti Undang-undang Nomor 36 Tahun 1999¹¹ tentang Telekomunikasi. Oleh karena itu sangat diharapkan semua kejahatan maya bisa ternetralkan dengan Undang-Undang tersebut, termasuk *defacing* yang sudah diatur ke dalamnya.

Dengan pesatnya perkembangan teknologi, hukum harus mampu beradaptasi dan memberikan perlindungan yang memadai terhadap ancaman kejahatan dunia maya. Oleh karena itu, penelitian ini akan menggali lebih dalam kerangka hukum yang mengatur peretasan di Indonesia, serta mengidentifikasi pertanggungjawaban pelaku peretasan situs web dalam konteks kejahatan digital. Dengan pemahaman yang lebih baik mengenai hal ini, agar penulis dapat membangun landasan yang lebih kuat untuk melindungi dan memahami aturan dan tindak pidana peretasan pada situs web kepada masyarakat Indonesia di era digital yang semakin kompleks ini. Hal ini menjadi salah satu alasan utama mengapa penulisan Tinjauan Yuridis Terhadap Tindak Pidana Pertanggungjawaban Tindak Pidana Peretasan Pada Situs Web Di Internet (*Defacing*) Berdasarkan Undang-Undang Nomor 1 Tahun 2024 Tentang Informasi dan Transaksi Elektronik perlu untuk dilakukan.

METODE PENELITIAN

Metode penelitian yang digunakan adalah penelitian hukum normatif (penelitian yuridis normatif). Dalam penelitian yuridis normatif ini penelitian dilakukan dengan cara menelaah bahan-bahan kepustakaan seperti teori, asas hukum, buku, atau jurnal penelitian terdahulu yang telah ada, serta peraturan perundang-undangan maupun doktrin-doktrin hukum yang berkaitan dengan penulisan penelitian. Pendekatan

¹⁰ Indonesia, Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.

¹¹ Indonesia, Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi.

penelitian hukum (*Approach*) yang digunakan dalam penelitian ini adalah Pendekatan Undang-Undang (*statute approach*) yang difokuskan pada Undang- Undang No. 1 Tahun 2024 Tentang perubahan kedua atas Undang-Undang No. 1 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Jenis data yang dipergunakan dalam penelitian ini adalah data sekunder yang diperoleh dari sumber bahan hukum. Pengumpulan bahan hukum dalam penulisan ini adalah dengan cara studi kepustakaan (*Library Research*). Metode analisis data yang dipergunakan adalah metode analisis kualitatif yaitu dengan cara mendalami serta membandingkan implementasi peraturan perundang-undangan dalam praktik.

HASIL DAN PEMBAHASAN

A.Tinjauan Yuridis Terhadap Pertanggungjawaban Tindak Pidana Peretasan Pada Situs Web Di Internet (*Defacing*) Berdasarkan Undang-Undang Nomor 1 Tahun 2024 Tentang Informasi Dan Transaksi Elektronik

1. Peretasan Pada Situs Web (*Defacing*)

Deface website merupakan tindakan yang dilakukan oleh seorang hacker atau peretas dengan tujuan untuk merusak atau mengubah tampilan *homepage* sebuah *website*. Tindakan ini sering dilakukan untuk menodai reputasi organisasi atau individu, mengeksploitasi kerentanan dalam sistem keamanan, atau menyampaikan pesan politik atau ideologis, biasanya yang terkena dampak dari defacing itu sendiri yaitu situs pemerintahan atau lembaga pelayanan publik karena dalam situs web pemerintahan atau lembaga pelayanan publik dapat mengundang audiens dengan sendirinya. Kejahatan dunia maya berupa perusakan situs web memiliki konsekuensi serius, baik bagi pemilik situs web maupun bagi pengguna yang mengandalkan informasi atau layanan yang dikandungnya. Selain itu, degradasi situs web juga dapat menjadi titik awal serangan

yang lebih berbahaya penyusupan ilegal ke dalam sistem situs web untuk tujuan memodifikasi konten atau mengubah tampilan beranda.¹²

Defacing terdiri dari dua tahap, yaitu mula-mula menerobos sistem orang lain atau kedalam web server seperti serangan *DDoS (Distributed Denial of Service)*, yang dimana membuat korban tidak dapat mengakses sistem, jaringan, atau TI lainnya yang mereka miliki. Seorang peretas ilegal atau kriminal umumnya menggunakan teknik serangan ini dengan tujuan merusak sistem, server web, dan juga mengganggu lalu lintas jaringan korban dengan serangan *DDOS*.¹³ atau serangan *malware* dan tahap kedua adalah mengganti halaman *website (web page)*. Antara *hacking* dan *defacing* tidak dapat terpisahkan satu sama lain, karena *defacing* merupakan salah satu kegiatan *hacking* yaitu, kegiatan menerobos program komputer milik orang atau pihak lain tanpa izin. Pada awalnya *hacking* tidak selalu berkonotasi negatif, karena sebenarnya tujuan *hacking* adalah untuk mengetahui sistem keamanan milik orang tertentu dan memberi tahu celahnya. Tetapi dalam perkembangannya di masyarakat *hacking* di nilai dan di anggap kata yang mewakili sebuah kejahatan dunia maya, dan pada kenyataanya memang *hacking* dilakukan tanpa izin.¹⁴

2. Pertanggungjawaban Tindak Pidana Peretasan Situs Web

Dalam bahasa Inggris, istilah untuk pertanggungjawaban pidana adalah *responsibility* atau *criminal liability*. Konsep mengenai pertanggungjawaban pidana sebenarnya tidak hanya berkaitan dengan hukum, tetapi juga berkaitan dengan nilai-nilai moral atau norma sosial yang diterima oleh suatu komunitas atau kelompok dalam masyarakat. Tujuannya adalah untuk memastikan bahwa pertanggungjawaban pidana

¹² Brian Budi Aji, Op. Cit, hlm 25-26.

¹³ Sari, Indah. "Menenal Hacking Sebagai Salah Satu Kejahatan Di Dunia Maya." *Jurnal Sistem Informasi Universitas Suryadarma* (Vol.10 No.2 2014), hlm 174.

¹⁴ Sutan Remi Syahdeini, *Kejahatan dan Tindak Pidana Komputer*, (Jakarta: Pustaka Utama Grafiti, 2009), hlm. 124.

dapat dicapai dengan cara yang memenuhi prinsip keadilan.¹⁵ Menurut Roeslan Saleh, tanggung jawab pidana dalam hukum positif di Indonesia dapat dijelaskan sebagai suatu elemen dari berlanjutnya tuduhan yang objektif yang terdapat dalam tindakan kriminal, dan secara subjektif telah memenuhi kriteria untuk diadili karena tindakan kriminal tersebut.¹⁶

Unsur tindakan adalah salah satu elemen utama dalam tanggung jawab pidana, karena seseorang tidak dapat dikenakan sanksi jika tidak melakukan suatu tindakan yang merupakan tindakan yang dilarang oleh hukum. Hal ini sejalan dengan prinsip legalitas yang dianut. Prinsip legalitas *nullum delictum nulla poena sine praevia lege poenali* berarti bahwa tidak ada sanksi bagi suatu tindakan jika tidak ada Undang-Undang atau peraturan yang mengatur larangan terhadap tindakan tersebut.¹⁷ Kesalahan yang dalam bahasa asing disebut dengan "*schuld*" merujuk pada kondisi psikologis individu yang berkaitan dengan tindakan yang telah dilakukannya sehingga berdasarkan keadaan itu, pelaku dapat dihakimi atas tindakannya.¹⁸

Pengaturan tindak pidana *defacing* dirumuskan dalam Undang-Undang Nomor 11 Tahun 2008 sebagaimana Undang-Undang tersebut telah diubah dengan Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik. Akan tetapi, sejarah penormaan pidana terhadap kejahatan *defacing* juga pernah dilakukan dengan menggunakan 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

¹⁵ Hanafi dan Mahrus, *Sistem Pertanggung Jawaban Pidana*, Cetakan pertama, Rajawali Pers (Jakarta: Rajawali Pers, 2015), hlm. 16.

¹⁶ Roeslan Saleh, *Perbuatan Pidana Dan Pertanggung jawaban Pidana* (Jakarta: Aksara Baru, 1980), hlm 75.

¹⁷ Moeljatno, *Asas-Asas Hukum Pidana*, Edisi revisi (Jakarta: Renika Cipta, 2008), hlm 25.

¹⁸ Afridus Darto, Arief Syahrul Alam, And Fifin Dwi Purwaningtyas, Pertanggungjawaban Pidana Bagi Pelaku Tindak Pidana Pembunuhan Pengidap Gangguan Kejiwaan Dalam Prespektif Hukum Pidana, *Jurnal Ilmu Hukum Wijaya Putra* (Vol.1 No. 2 2023), hlm 4.

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*.

Lahirnya Undang-Undang Nomor 11 Tahun 2008 juncto Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik sebagai hukum pidana khusus dalam menangani perkara tindak pidana defacing, maka sesuai *asas lex specialis derogate legi generali*, undang-undang ini telah mengesampingkan ketentuan penghancuran dan pengrusakan barang dalam Pasal 406 ayat (1) KUHP yang sebelumnya digunakan untuk mengisi kekosongan hukum terkait tindak pidana defacing. Selain itu, dengan disahkannya Undang-Undang Nomor 11 Tahun 2008 juncto Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik sebagai hukum terbaru menurut *asas lex posterior derogate legi priori* telah mengesampingkan ketentuan tentang tindak pidana defacing dalam Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi. Dengan demikian, setiap perkara tindak pidana defacing yang saat ini terjadi diselesaikan berdasarkan ketentuan dalam Undang-Undang Nomor 11 Tahun 2008 juncto Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik.¹⁹

Undang-Undang Republik Indonesia 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 Undang-Undang Informasi dan Transaksi Elektronik mengenai perbuatan defacing termasuk ke dalam perbuatan yang dilarang yang apabila dilihat dari tahap awal melakukan defacing yaitu melakukan

¹⁹ Diana et al., "Analisis Kriminologis Defacing Dalam Bentuk Cyber Crime." *Prosiding Snapp: Sosial Humaniora, Pertanian, Kesehatan Dan Teknologi* (Vol.2 No.1 2023): 211-220.

Illegal access, bahwa *illegal access* telah diatur pada Pasal 30 ayat (1), (2) dan (3).²⁰ 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, menerobos, melampaui, atau menjebol sistem pengamanan.²¹

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. Pasal tersebut menyebutkan mengenai larangan untuk melakukan modifikasi/pengubahan terhadap suatu *website* maupun tergolong ke dalam kategori data *interference* yang ada pada bab tentang perbuatan dilarang, seperti yang dikatakan sebelumnya bahwa

²⁰ Lani Zihan Ayustin, "Perbuatan Pidana Mengakses Tanpa Hak ke Sistem Elektronik Orang Lain Menurut Undang-Undang No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik," *Jurnal Ilmiah Mahasiswa Hukum (JIMHUM)* (Vol.2 No.3 2022), hlm 3.

²¹ Indonesia, Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.

ada dua tahap dalam melakukan *defacing*, pertama melakukan hacking dan selanjutnya memodifikasi *website*.²²

Defacing yang tergolong ke dalam tindak pidana perusakan dan penghancuran secara umum (*lex generalis*) diatur dalam Kitab Undang-Undang Hukum Pidana, tetapi secara khusus (*lex specialis*) *defacing* yang merupakan kejahatan di dunia maya dengan menggunakan sarana teknologi informasi dalam melancarkan aksinya ini diatur dalam Undang-Undang Nomor 11 Tahun 2008 jo. Undang Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik (UU ITE). Pemidanaan pelaku tindak pidana *defacing* apabila berdasarkan *asas lex specialis derogat legi generali*, maka ketentuan yang digunakan hanya ketentuan yang bersifat khusus (*lex specialis*) yaitu ketentuan yang termuat dalam Undang Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik. Adanya batasan norma dalam Undang Undang Informasi dan Transaksi Elektronik (ITE) yang berkaitan dengan tindak pidana *defacing* terdapat dalam Pasal 30 ayat (1), ayat (2), ayat (3), Pasal 32 ayat (1).²³

Adapun terkait Pasal 30 Undang-Undang Informasi dan Transaksi Elektronik, apabila melihat Undang-Undang Nomor 1 Tahun 2023 Tentang Kitab Undang-Undang Hukum Pidana (KUHP) terbaru yang akan berlaku di tahun 2026, menurut Pasal 622 Undang-Undang Nomor 1 Tahun 2023 yaitu:

(1) Pada saat Undang-Undang ini mulai berlaku, ketentuan dalam yang tertulis di huruf r menyebutkan bahwa salah satu pasal dari undang-undang informasi dan transaksi elektronik yaitu pasal 30 dicabut dan dinyatakan tidak berlaku.

Dan diubah menjadi pasal Pasal 333 Dipidana dengan pidana penjara paling lama 7 (tujuh) tahun atau pidana denda paling banyak kategori VI, Setiap Orang yang:

a. tanpa hak menggunakan atau mengakses Komputeratau sistem elektronik dengan cara apa pun, denganmaksud memperoleh, mengubah,

²² J. R. Dyda and E. Ratnawati, "Pengaturan Tindak Pidana Cyber Crime dalam Hukum Positif di Indonesia," *Gorontalo Law Revie*" (Vol. 6 No. 2 2023), hlm 243–252.

²³ Diana et al Op. Cit., hlm 217.

merusak, atau menghilangkan informasi pertahanan nasional atau hubungan internasional yang dapat menyebabkan gangguan atau bahaya terhadap negara atau hubungan dengan subjek hukum internasional;

b. tanpa hak melakukan tindakan yang menyebabkan transmisi dari program, informasi, kode atau perintah Komputer atau sistem elektronik yang dilindungi negara menjadi rusak;

c. tanpa hak atau melampaui wewenangnya menggunakan atau mengakses Komputer atau sistem elektronik, baik dari dalam maupun luar negeri untuk memperoleh

informasi dari Komputer atau sistem elektronik yang dilindungi oleh negara;

d. tanpa hak menggunakan atau mengakses Komputer atau sistem elektronik milik pemerintah;

e. tanpa hak atau melampaui wewenangnya menggunakan atau mengakses Komputer atau sistem elektronik yang dilindungi oleh negara, yang mengakibatkan Komputer atau sistem elektronik tersebut menjadi rusak;

f. tanpa hak atau melampaui wewenangnya menggunakan atau mengakses Komputer atau sistem elektronik yang dilindungi oleh masyarakat, yang mengakibatkan Komputer atau sistem elektronik tersebut menjadi rusak;

g. memengaruhi atau mengakibatkan terganggunya Komputer atau sistem elektronik yang digunakan oleh pemerintah;

h. menyebarkan, memperdagangkan, atau memanfaatkan Kode Akses atau informasi yang serupa dengan hal tersebut, yang dapat digunakan menerobos Komputer atau sistem elektronik dengan tujuan menyalahgunakan Komputer atau sistem elektronik yang digunakan atau dilindungi oleh pemerintah; atau

i. melakukan perbuatan dalam rangka hubungan internasional dengan maksud merusak Komputer atau sistem elektronik lainnya yang dilindungi

negara dan berada di wilayah yurisdiksi Indonesia dan ditujukan kepada siapa pun.²⁴

B. Penegakan Hukum Terhadap Pelaku Tindak Pidana Peretasan Situs Web Yang Dilakukan Di Internet (*Defacing*) ?

1. Sanksi terhadap Pelaku Tindak Pidana Peretasan Situs Web (*Defacing*)

Adapun ketentuan pidana dari pasal-pasal tersebut diatas mengenai tindak kejahatan mengakses komputer dan/atau Sistem elektronik milik Orang lain dengan cara apa pun (*illegal acces*) diatur dalam BAB XI Ketentuan Pidana dalam Undang-Undang No.11 Tahun 2008 jo Undang-Undang No.1 Tahun 2024 Tentang Informasi dan Transaksi Elektronik yaitu Pasal 46 yang berbunyi:

1. Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/ atau denda paling banyak Rp.600.000.000,00 (enam ratus juta rupiah).
2. Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam pasal 30 ayat (2) dipidana dengan pidana penjara paling lama 7 (tujuh) tahun dan/ atau denda paling banyak Rp.700.000.000,00 (tujuh ratus juta rupiah).
3. Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam pasal 30 ayat (3) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/ atau denda paling banyak Rp.800.000.000,00 (delapan ratus juta rupiah).²⁵

Ketentuan pidana dari pasal 32 mengenai tindak kejahatan Peretasan situs web (*Defacing*) diatur juga dalam BAB XI Ketentuan Pidana dalam UU NO.11 Tahun 2008 jo UU No.1 Tahun 2024 Tentang Informasi dan Transaksi Elektronik yaitu: Pasal 48 yang berbunyi:

- (1) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (1) dipidana dengan pidana penjara paling lama 8 (delapan)

²⁴ Indonesia, Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana.

²⁵ Ibid

tahun dan/atau denda paling banyak Rp2.000.000.000,00 (dua miliar rupiah).²⁶

2. Penegakan Hukum Terhadap Pelaku Tindak Pidana *Defacing*

Salah satu komponen penegakan hukum adalah penegak hukum. Orang-orang yang berkontribusi pada proses penegakan hukum disebut penegak hukum, baik secara langsung maupun tidak langsung. Pada dasarnya, penegak hukum akan menggabungkan prinsip-prinsip, dan tindakan. Tindakan dan pemeliharaan biasanya dilakukan oleh penegak hukum untuk mencapai tujuan keadilan. Dalam melaksanakan tugasnya, penegak hukum seringkali membuat keputusan tentang masalah yang dihadapi; namun, mereka harus tetap berpegang teguh pada peraturan saat membuat keputusan, karena aturan mengenai masalah tersebut belum ada.²⁷

Di Indonesia aparat penegak hukum yang memiliki kewenangan dalam menangani perkara

tindak pidana cyber crime hacker dibagi menjadi 3 yaitu ;

1. Pengadilan

Pengadilan sebagai instansi resmi negara bertugas untuk melakukan pemeriksaan, memberikan keadilan dengan cara mengadili, memberikan putusan, dan menyelesaikan segala perkara atau permasalahan yang diajukan oleh warga masyarakat. Perkara yang diselesaikan melalui pengadilan akan dapat berjalan sebagaimana mestinya jika semua pihak yang berada atau ikut didalam penyelesaian perkara tersebut. Para pihak yang berperkara atau dari hakimnya sendiri harus mengikuti aturan main (*rule of game*) secara jujur dan sesuai dengan peraturan yang ada.

Pihak yang mengajukan perkara di pengadilan tentunya mempunyai maksud untuk mendapatkan penyelesaian dan pemecahan perkara secara adil dan sesuai dengan harapan dan keinginan para pihak pencari keadilan (*justiciabellen*). Untuk mendapatkan penyelesaian

²⁶ Ibid

²⁷ Soekanto S, *Polisi Dan Lalu Lintas* (Analisis Menurut Sosiologi Hukum)., (Bandung: Mandar Maju, 1990), hlm 6.

perkara secara adil dan sesuai dengan harapan dan keinginan para pihak pencari keadilan harus melalui proses pembuktian. Proses tersebut bertujuan untuk mengetahui duduk perkara secara jelas, yaitu peristiwa yang benar dan peristiwa yang salah.

Di dalam proses pembuktian para pihak diberikan kesempatan untuk mengemukakan pendapat mengenai peristiwa yang terjadi. Hal tersebut sangat penting karena sebagai dasar untuk meneguhkan hak dan membantah hak dari pihak lain. Dalam hal mengemukakan pendapat para pihak tidak cukup sekedar memberikan pendapatnya secara lisan maupun tertulis saja, tetapi harus didukung dan disertai dengan bukti-bukti yang sah menurut hukum agar kebenarannya dapat dipastikan.²⁸

2. Kejaksaan

Kejaksaan adalah lembaga pemerintahan yang melaksanakan kekuasaan negara dibidang penuntutan serta kewenangan lain berdasarkan undang-undang. Selain itu kejaksaan merupakan lembaga non departemen, yang berarti kejaksaan tidak berada dibawah kementerian apapun. Kejaksaan dipimpin oleh Jaksa Agung, dimana nantinya Jaksa Agung yang memiliki tanggung jawab terhadap presiden. Tanggung jawab tersebut menjadikan Jaksa Agung memiliki kedudukan setingkat dengan Menteri. Jaksa Agung memimpin kejaksaan yang terbagi ke dalam beberapa daerah hukum mulai dari ingkat Provinsi (jaksa tinggi) sampai dengan tingkat Kabupaten (kejaksaan negeri) di seluruh wilayah Indonesia.

Kejaksaan memiliki tugas utama sebagai salah satu lembaga penegak hukum dalam sistem peradilan pidana Indonesia. Adapun tugasnya untuk melakukan penuntutan dan sebaliknya. Penuntutan merupakan kewenangan satu-satunya yang hanya dimiliki oleh kejaksaan dan tidak dimiliki oleh lembaga penegak hukum lain. Dalam melaksanakan fungsi, tugas, dan wewenanganya, kejaksaan terlepas dari

²⁸ Arisandy, Yogi Oktafian. "Penegakan Hukum terhadap Cyber Crime Hacker." *Indonesian Journal of Criminal Law and Criminology (IJCLC)* (Vol.1 No.3 2020), hlm 162-169.

segala pengaruh kekuasaan pemerintah, dan pengaruh dari kekuasaan lainnya. Negara memberikan jaminan kepada jaksa di dalam menjalankan profesinya tanpa adanya intimidasi, gangguan, godaan, dan campur tangan yang tidak sesuai atau pembeberan dari segala sesuatu yang belum teruji kebenarannya, baik terhadap pertanggungjawaban perdata, pidana, maupun lainnya.²⁹

3. Kepolisian

Kepolisian merupakan salah satu dari aparat penegak hukum. Tugas dari aparat kepolisian yaitu memelihara keamanan dan ketertiban masyarakat, menegakkan hukum, memberikan perlindungan, pengayoman dan pelayanan terhadap masyarakat. Segala aturan mengenai fungsi kepolisian sendiri sudah diatur didalam Undang-Undang No. 2 Tahun 2002 tentang Kepolisian Negara Republik Indonesia. Peraturan tersebut menjelaskan bahwa salah satu fungsi kepolisian adalah menjalankan fungsi pemerintahan negara yang memberikan perlindungan, mewujudkan atau menjaga ketertiban, memberikan pelayanan dan pengayoman terhadap masyarakat, serta melakukan penegakan hukum. Hal tersebut jelas disebutkan didalam Pasal 14 ayat (1) Undang-Undang Kepolisian.

Dalam kasus pidana pada umumnya polisi akan langsung bertindak melakukan penyidikan meskipun tidak ada laporan atau aduan terlebih dahulu. Akan tetapi hal tersebut tentunya memerlukan berbagai pertimbangan terlebih dahulu. Tindakan penyidikan tersebut merupakan tugas dari kepolisian sebagaimana disebutkan didalam Pasal 14 ayat (1) huruf g yang menyatakan bahwa polisi berwenang melakukan penyidikan tindakan pidana sesuai dengan hukum acara pidana dimana sebelumnya didahului oleh tindakan penyelidikan oleh penyidik.³⁰

Dalam hal melakukan penegakan hukum khususnya dalam bidang kejahatan mayantara, kejahatan ini memiliki jangkauan yang sangat luas tanpa mengenal batas wilayah teritorial suatu negara karena kejahatan

²⁹ Ibid

³⁰ Arisandy, Yogi Oktafian Op.Cit., hlm 165.

ini bersifat transnasional. Tipe kejahatan yang tak mengenal batas ini mengharuskan yurisdiksi suatu negara terlibat langsung di dalamnya karena sangat jauh dari jangkauan suatu negara. Jika tanpa melakukan kerja sama antar negara dalam melakukan pemberantasan serta penegakan hukum yang sebagaimana mestinya, kejahatan yang bersifat transnasional ini akan menimbulkan masalahnya sendiri berkenaan dengan yurisdiksi.³¹

Seringkali masalah ini menjadi sangat pelik karena kendala sebuah teritorial batas negara. Yurisdiksi dalam hal ini telah mencakup dan bertanggungjawab atas orang, benda atau peristiwa hukum yang terjadi didalamnya. Hukum Internasional telah membagi beberapa prinsip yang dapat menjadi acuan dalam masalah yurisdiksi yakni prinsip teritorial, prinsip nasionalitas, prinsip perlindungan, serta prinsip universal, yaitu :

1. Prinsip teritorial: 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.³²

Salah satu cara yang dapat dilakukan oleh negara yang memiliki yurisdiksi terhadap pelaku kejahatan yang berada di negara lain adalah dengan meminta kepada negara di tempat pelaku tersebut berada agar

³¹ Dikdik M. Arief Mansur dan Elisatris Gultom Op. Cit., hlm 49.

³² I. Gusti Ayu Suanti Karnadi et al., "Penegakan Hukum terhadap Tindak Pidana Peretasan sebagai Bentuk Kejahatan Mayantara (Cyber Crime)." *Jurnal Konstruksi Hukum* (Vol.1 No.2 2020), hlm 334-339.

dapat menangkap pelaku tersebut. Yurisdiksi terhadap kejahatan mayantara (cybercrime) khususnya dalam tindak pidana peretasan (hacking) dapat dilaksanakan melalui kerja sama internasional berupa ekstradisi, bantuan hukum timbal balik, dan kerjasama antar penegak hukum.³³

Mengenai ruang lingkup berlakunya pasal 2 undang-undang nomor 1 tahun 2024 mengatur terkait tindak pidana *defacing* yaitu berlaku untuk setiap orang yang melakukan perbuatan hukum sebagaimana diatur dalam Undang-Undang ini, baik yang berada di wilayah hukum Indonesia maupun di luar wilayah hukum Indonesia, yang memiliki akibat hukum di wilayah hukum Indonesia dan/atau diluar wilayah hukum Indonesia dan merugikan kepentingan Indonesia.³⁴

3. Hambatan Penegakan Hukum Terhadap Pelaku Tindak Pidana *Cybercrime*

Penegakan kejahatan siber di Indonesia menghadapi berbagai tantangan teknis yang menghambat efektivitas penegakan hukum. Tantangan teknis ini meliputi:

- a. Keterbatasan sumber daya manusia.
- b. Keterbatasan peralatan dan infrastruktur teknis.
- c. Kompleksitas bukti digital.
- d. Keterbatasan kerja sama internasional.

Salah satu kendala utama adalah terbatasnya sumber daya manusia (SDM) dengan keahlian khusus dalam forensik digital. Penyidik sering kali tidak dibekali dengan pengetahuan atau pelatihan yang memadai untuk menangani bukti digital, seperti analisis log aktivitas, pelacakan alamat IP, atau mendekripsi data terenkripsi. Dalam banyak kasus, penegakan hukum membutuhkan keahlian tingkat lanjut untuk membongkar sistem rumit yang digunakan oleh pelaku, seperti penggunaan jaringan anonim (web gelap) atau transaksi mata uang kripto yang sulit dilacak. Selain keterbatasan sumber daya manusia, peralatan

³³ Ibid

³⁴ Ibid

teknis dan infrastruktur untuk mendukung investigasi sering kali tidak memadai. Alat analisis forensik digital tingkat lanjut, seperti perangkat lunak pelacakan data atau alat pemulihan data yang dihapus, masih langka atau tidak tersedia di banyak wilayah.³⁵

Penindakan kasus cyber crime sering mengalami hambatan terutama dalam penangkapan tersangka dan penyitaan barang bukti. Dalam penangkapan tersangka, sering kali tidak dapat menentukan secara pasti siapa pelakunya karena mereka melakukannya cukup melalui komputer yang dapat dilakukan dimana saja tanpa ada yang mengetahuinya, sehingga tidak ada saksi yang mengetahui secara langsung. Hasil pelacakan paling jauh hanya dapat menemukan IP Address dari pelaku dan komputer yang digunakan. Hal itu akan semakin sulit apabila menggunakan warnet sebab saat ini masih jarang sekali warnet yang melakukan registrasi terhadap pengguna jasa mereka sehingga kita tidak dapat mengetahui siapa yang menggunakan komputer tersebut pada saat terjadi tindak pidana.³⁶

Hal ini membuat proses penyelidikan menjadi lambat dan kurang akurat, terutama ketika bukti digital memerlukan penanganan segera untuk mencegah kehilangan data akibat manipulasi atau batas waktu penyimpanan. Kendala teknis lainnya adalah kompleksitas bukti digital yang sering kali tersebar di berbagai platform global. Penyidik harus berhadapan dengan sistem keamanan tinggi yang diterapkan oleh layanan cloud atau platform media sosial, yang sering kali berbasis di luar negeri. Situasi ini menuntut kerjasama internasional, yang tidak selalu mudah diperoleh, terutama jika platform itu ada di negara tanpa perjanjian kerjasama hukum dengan Indonesia. Selain itu, bukti digital bersifat mudah dimanipulasi atau dihapus, sehingga memerlukan

³⁵ Muhammad Singgih Imam Wibowo, Akhmad Munawar. "Kendala teknis dan hukum dalam proses penyidikan tindak pidana siber di Indonesia." *Jurnal Hukum Lex Generalis* (Vol.5 No.7 2024), hlm 4.

³⁶ Ibid

tindakan cepat dan akurat, yang sering kali menjadi tantangan teknis tersendiri bagi aparat penegak hukum.³⁷

KESIMPULAN

Dapat Disimpulkan bahwa Defacing merupakan salah satu cybercrime yang tindakannya merupakan dilakukan oleh seorang hacker atau peretas untuk merusak atau mengubah tampilan homepage sebuah website dengan tujuan menodai reputasi organisasi/pemerintahan atau individu, mengeksploitasi kerentanan dalam sistem keamanan, atau menyampaikan pesan politik atau ideologis. Praktik Defacing saat ini diatur dalam Undang-undang no 1 Tahun 2024 yang dimana memberikan sanksi berupa membayar denda serta hukuman kurungan penjara sebagaimana telah dicantumkan dalam pasal 30 ayat (1), (2), dan (3). Sanksi pidananya telah diatur dalam pasal 46 ayat (1),(2), dan (3).

Penegakan Hukum di Indonesia terkait cybercrime khususnya defacing seringkali mengalami hambatan terutama dalam penangkapan tersangka dan penyitaan barang bukti. Dalam penangkapan tersangka sering kali tidak dapat menentukan secara pasti siapa pelakunya karena mereka melakukannya cukup melalui komputer yang dapat dilakukan dimana saja tanpa ada yang mengetahuinya sehingga tidak ada saksi yang mengetahui secara langsung

SARAN

Pemerintah harus melakukan perbaikan dan penyesuaian terkait peraturan perundang-undangan tidak hanya tindak pidana defacing akan tetapi kejahatan-kejahatan baru yang muncul di era digital yang berkembang semakin kompleks, meningkatkan koordinasi antar lembaga penegak hukum, dan meningkatkan kemampuan sumber daya manusia melalui pelatihan teknis. Diharapkan bahwa langkah-langkah strategis yang komprehensif ini akan meningkatkan efisiensi dan efektivitas penyidikan tindak pidana siber di Indonesia dan membuatnya sesuai dengan standar hukum internasional yang berlaku.

³⁷ Muhammad Singgih Imam Wibowo Op.Cit., hlm 5.

DAFTAR PUSTAKA**1. Buku**

- Budi Suhariyanto, Tindak Pidana Teknologi Informasi (CyberCrime): Urgensi Pengaturan dan Celah Hukumnya, Jakarta: Rajawali Pers, 2014.
- Deni, D., & Hendra, P. D. Desain dan Pemrograman Website, Bandung: PT Remaja Rosdakarya, 2013.
- Hanafi dan Mahrus, Sistem Pertanggung Jawaban Pidana, Cetakan pertama, Jakarta: Rajawali Pers, 2015.
- Mansur, D. M. A. Cyber law: aspek hukum teknologi informasi, Bandung: Refika Aditama, 2009.
- Moeljatno, Asas-Asas Hukum Pidana, Edisi revisi, Jakarta: Renika Cipta, 2008.
- Roeslan Saleh, Perbuatan Pidana Dan Pertanggung jawaban Pidana, Jakarta: Aksara Baru, 1980.
- Soekanto S, Polisi Dan Lalu Lintas (Analisis Menurut Sosiologi Hukum). Bandung: Mandar Maju, 1990.
- Syahdeini, Sutan Remi, Kejahatan dan Tindak Pidana Komputer, Jakarta: Pustaka Utama Grafiti, 2009.
- Tahir, Rusdin et al., Metodologi Penelitian Bidang Hukum: Suatu Pendekatan Teori Dan Praktik, Jambi: Pt. Sonpedia Publishing Indonesia, 2023.
- Wahid, Abdul dan Mohammad Labib, Kejahatan Mayantara (Cyber Crime), Bandung: Refika Aditama, 2010.

2. Artikel Jurnal

- Afridus Darto, Arief Syahrul Alam, And Fifin Dwi Purwaningtyas, Pertanggungjawaban Pidana Bagi Pelaku Tindak Pidana Pembunuhan Pengidap Gangguan Kejiwaan Dalam Prespektif Hukum Pidana, Jurnal Ilmu Hukum Wijaya Putra (Vol.1 No. 2 2023).
- Aji, Brian Budi, Tindakan Kejahatan Cyber Crime Dalam Bentuk Deface Website: Cyber Security Dan Forensik Digital, Jurnal Universitas Islam Negeri Sunan Kalijaga (Vol. 6 No. 1 2023).
- Arisandy, Yogi Oktafian. "Penegakan Hukum terhadap Cyber Crime Hacker." Indonesian Journal of Criminal Law and Criminology (IJCLC) (Vol.1 No.3 2020).
- Diana et al., "Analisis Kriminologis Defacing Dalam Bentuk Cyber Crime." Prosiding Snapp: Sosial Humaniora, Pertanian, Kesehatan Dan Teknologi (Vol.2 No.1 2023).
- I. Gusti Ayu Suanti Karnadi et al., "Penegakan Hukum terhadap Tindak Pidana Peretasan sebagai Bentuk Kejahatan Mayantara (Cyber Crime)." Jurnal Konstruksi Hukum (Vol.1 No.2 2020)

- Sari, Indah. "Mengenal Hacking Sebagai Salah Satu Kejahatan Di Dunia Maya." Jurnal Sistem Informasi Universitas Suryadarma (Vol.10 No.2 2014)
- J. R. Dyda and E. Ratnawati, "Pengaturan Tindak Pidana Cyber Crime dalam Hukum Positif di Indonesia," Gorontalo Law Review" (Vol. 6 No. 2 2023).
- Zihan, Lani Ayustin, "Perbuatan Pidana Mengakses Tanpa Hak ke Sistem Elektronik Orang Lain Menurut Undang-Undang No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik," Jurnal Ilmiah Mahasiswa Hukum (JIMHUM) (Vol.2 No.3 2022).
- Wibowo, Muhammad Singgih Imam , Akhmad Munawar. "Kendala teknis dan hukum dalam proses penyidikan tindak pidana siber di Indonesia." Jurnal Hukum Lex Generalis (Vol.5 No.7 2024).

3. Peraturan Perundang-Undangan

- Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana (KUHPidana terbaru)
- Undang-Undang Republik Indonesia No 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik (UU ITE).
- Undang-Undang Republik Indonesia No 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik (UU ITE).
- Undang-Undang Republik Indonesia Nomor 1 Tahun 1946 Tentang Kitab Undang-Undang Hukum Pidana (KUHPidana).
- Undang-Undang Republik Indonesia Nomor 36 Tahun 1999 Tentang Telekomunikasi.

CV PENULIS



Penulis bernama lengkap Fariddudin Imam Hastomo. Tempat dan tanggal lahir Bekasi, 10 Juni 2003, beragama Islam. Penulis anak ke dua dari tiga bersaudara. Menyelesaikan pendidikan formalnya pada SDN Jatimakmur 1 (2009-2015), SMP 23 Bekasi (2015-2018), dan SMA 21 Bekasi (2018-2021). Pada tahun 2021 penulis melanjutkan pendidikannya dan terdaftar sebagai mahasiswa pada Fakultas Hukum Universitas Dirgantara Marsekal Suryadarma.