E-ISSN: 3031-0458

Indonesian Journal of Islamic Jurisprudence,Economic and Legal Theory

Analisis Pengaturan Hukum Terhadap Kejahatan Siber Doxing Di Indonesia

Diaz Marsillo Prisdallini[1], Andrie Irawan[2]
[1,2] Universitas Surakarta
Email : diazmarsillo207@gmail.com[1], andrie.ir@gmail.com[2]

Received 28-06-2024| Revised form 29-07-2024 | Accepted 11-08-2024

Abstract

The idea of conducting research related to "Reconstruction of Doxing Cybercrime Regulation in Indonesia", is based on the purpose of knowing; first, what is the background for the emergence of cybercrime, especially doxing cybercrime in Indonesia?; second, to what extent do state institutions in charge of legislative affairs respond to problems (social and legal) due to the development of cybercrime doxing in Indonesia, so that law enforcement officials can anticipate and overcome them?; Third, how can the regulation of cybercrime doxing in Indonesia be reconstructed, so that it can be a solution to the problems that occur? The research method used is a normative juridical method with a legislative approach, a conceptual approach, and a case approach. The results of the study show that: (1) The reality of cybercrime must be observed first from the parent of cybercrime, namely; Cyberspace which is a new reality in human life, identification begins with; (a) analysis of the occurrence of social change as an impact of the development of technological innovation, (b) innovation is an alternative approach for humans as social creatures in interacting, (c) this social interaction forms a newcommunity in the form of a virtual form, namely cybercommunity (cybercommunity/cybersociety), (d) currently a new form of cybercrime has emerged called doxing, which is a violation of the right to personal data. (2) Regulatory readiness in anticipating and overcoming cybercrime, especially doxing cybercrime in Indonesia, begins with; (a) analysis of general regulations on cybercrime, (b) analysis of special regulations on cybercrime, and (c) analysis of problems in cybercrime regulations, especially doxing cybercrime. As a complement to the results of this study, it is recommended to state administrators to respond to the development of cybercrime doxing by reconstructing the current laws and regulations.

Keywords: *Regulation, Crime, Cyber Doxing*

Abstrak

Gagasan melakukan penelitian terkait "Rekonstruksi Pengaturan Kejahatan Siber Doxing di Indonesia", didasarkan kepada tujuan untuk mengetahui; pertama, apa yang melatarbelakangi timbulnya kejahatan siber, khususnya kejahatan siber doxing di Indonesia?; kedua, sejauhmana lembaga negara yang membidangi urusan legislasi menyikapi problematika (sosial maupun hukum) akibat berkembangnya kejahatan siber doxing di Indonesia, sehingga aparat penegak hukum dapat mengantisipasi dan mengatasinya?; ketiga, bagaimana sejatinya pengaturan kejahatan siber doxing di

Indonesia direkonstruksi, sehingga dapat menjadi solusi atas permasalahan yang terjadi? Metode penelitian yang digunakan adalah metode yuridis normatif dengan pendekatan perundang-undangan, pendekatan konseptual, pendekatan kasus. Hasil dari penelitian memperlihatkan, bahwa: (1) Realita kejahatan siber (cybercrime) harus dicermati terlebih dahulu dari induk kejahatan siber, yaitu; ruang maya (cyberspace) yang merupakan realita baru dalam kehidupan manusia, identifikasi diawali dengan; (a) analisis terjadinya perubahan sosial sebagai dampak dari perkembangan inovasi teknologi, (b) inovasi menjadi pendekatan alternatif bagi manusia sebagai mahkluk sosial dalam berinteraksi, (c) interaksi sosial ini membentuk suatu komunitas baru yang berwujud virtual, yaitu masyarakat siber (cybercommunity/ cybersociety), (d) saat ini muncul bentuk kejahatan siber baru yang disebut doxing, yaitu pelanggaran hak atas data pribadi. (2) Kesiapan regulasi dalam mengantisipasi dan mengatasi kejahatan siber khususnya kejahatan siber doxing di Indonesia, diawali dengan; (a) analisis regulasi umum atas tindak kejahatan siber, (b) analisis regulasi khusus atas tindak kejahatan siber, dan (c) analisis problematika regulasi kejahatan siber khususnya kejahatan siber doxing. Sebagai pelengkap dari hasil penelitian ini, maka direkomendasikan kepada penyelenggara negara agar memberi respon atas berkembangnya kejahatan siber doxing dengan melakukan rekonstruksi peraturan perundang-undangan yang ada saat ini.
Kata Kunci: Pengaturan, Kejahatan, Siber Doxing

PENDAHULUAN

Kejahatan siber merupakan kejahatan yang mempunyai karakteristik tersendiri yang berbeda dengan kejahatan tradisional pada umumnya. Perbedaan yang mencolok adalah terletak pada modus dan sarana kejahatan. Oleh karena kekhasan sifatnya tersebut, maka pemberantasan kejahatan ini harus dilakukan dengan cara yang berbeda yang mengikuti perkembangan teknologi informasi.

Pandangan kejahatan siber doxing sebagai suatu perbuatan yang dilakukan seseorang untuk bisa mendapatkan data atau identitas pihak lain dengan tujuan memperoleh keuntungan materi (ekonomi), mendapatkan perhatian dan atau pengakuan, atau bahkan untuk tujuan kepentingan politik, setidaknya didukung dengan laporan riset Data Breach Investigation Report (DBIR) tahun 2022 yang menjelaskan, bahwa dari seluruh kasus pencurian data global pada tahun 2021, sebanyak 96% kasus dilatarbelakangi motif finansial, 3% kasus bermotif protes sosial atau hacktivism, 2% dilatarbelakangi oleh kehendak bersenang-senang atau iseng, dan 1% karena dendam pribadi.

Bersandar kepada perbuatan melawan hukum tersebut, maka timbul kemudian keresahan, kecemasan, dan ketakutan masyarakat akan ancaman hilangnya harta benda, harkat dan martabat, hingga jiwa yang dimilikinya, sehingga masyarakat memandang

perlu untuk memperoleh perlindungan dari penyelenggara negara, khususnya aparat penegak hukum. Akan tetapi fakta memperlihatkan, bahwa sejumlah warga masyarakat yang pernah menjadi korban atas kejahatan siber doxing tersebut belum sepenuhnya merasa mendapatkan jaminan kepastian hukum, karena kurang terakomodirnya instrumen (legal standing) yang dapat dijadikan landasan pemidanaan, meskipun sudah ada Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) serta Undang-Undang Perlindungan Data Pribadi (UU PDP).

Merespon keadaan tersebut, maka lembaga legislatif dipandang perlu untuk merekonstruksi pengaturan terhadap kejahatan siber doxing, dalam hal ini Undang-Undang Informasi dan Transaksi Elektronik maupun Undang- Undang Perlindungan Data Pribadi atau membuat penemuan hukum atas kejahatan yang belum diatur. Semua jenis kejahatan ini sesungguhnya sudah diatur dalam tindakan kriminal lainnya, yang kemudian hal ini menciptakan apa yang disebut Douglas Huzak sebagai kriminalisasi berlebihan.

Penemuan hukum, menurut Sudikno Mertokusumo, Guru Besar Ilmu Hukum Universitas Gadjah Mada, adalah proses pembentukan hukum oleh hakim atau petugas hukum lainnya yang diberi tugas melaksanakan hukum terhadap peristiwa-peristiwa konkret. Penemuan hukum adalah konkretisasi, kristalisasi atau individualisasi peraturan hukum (das sollen) yang bersifat umum dengan mengingat peristiwa konkret (das sein). Lebih lanjut menurut Sudikno, peristiwa konkret perlu dicarikan hukumnya yang bersifat umum dan abstrak. Peristiwa konkret harus dipertemukan dengan peraturan hukum. Peristiwa konkret harus dihubungkan dengan peraturan hukumnya agar dapat tercakup oleh peraturan hukum itu. Sebaliknya, peraturan hukumnya harus disesuaikan dengan peristiwa konkretnya agar dapat diterapkan.

Hal senada juga disampaikan oleh Sabian Utsman dalam bukunya Metodologi Penelitian Hukum Progresif, das sollen dan das sein ditemukan dalam penelitian hukum. Penelitian hukum setidaknya mendiskusikan antara apa yang seharusnya hukum sebagai fakta hukum (das sollen) yang diungkapkan para ahli hukum dalam tataran teoritik (lawin the books), pada tataran ini lebih pada kajian dasar-dasar normatif (hukum dalam bentuk cita- cita bagaimana seharusnya) dengan apa yang senyatanya (das sein) lebih kepada hukum sebagai fakta, yaitu hukum yang hidup berkembang dan berproses di masyarakat (law in action).

Tindak Pidana Siber diatur dalam Bab VII Pasal 27 sampai Pasal 37 UU ITE. Di dalam undang-undang ini disebutkan dengan tegas bahwa tindak pidana yang ada di dalamnya adalah segala tindak kejahatan berupa pelanggaran atas "Perbuatan Terlarang" yang ada di dalam undang-undang tersebut. Kasus kejahatan siber doxing sesungguhnya dapat dijerat dengan UU-ITE Pasal 26 aya1 1 dan ayat 2, tetapi konstruksi dari pasal tersebut sulit untuk diterapkan pada kondisi nyata dan merupakan problematika hukum saat ini. Beberapa yang menjadi perhatian adalah: (1) Pasal 26 dari UU-ITE bukan merupakan pasal pelanggaran atas Perbuatan Terlarang, dan (2) Pasal 26 ayat 2 menyatakan bahwa pelanggaran atas data pribadi seseorang harus ditunjukkan dengan "kerugian" yang bersifat materiil. Selain itu terdapat hal prinsipil berupa azas legalitas (KUHP Pasal 1 ayat 1) yang tidak dapat dipenuhi oleh UU-ITE pasal 26 sebagai dasar pemidanaan.

Ketiadaan dasar pemidanaan tersebut menyebabkan kejahatan siber doxing kini

telah menjadi problematika sosial sebagai akibat tren kejahatan siber dan perubahan perilaku bisnis, bahkan telah menjadi problematika hukum baik di Indonesia dan negara-negara lain. Hal ini ditunjukkan dengan realita kejahatan siber doxing di Indonesia saat ini telah memasuki tahap yang mengkhawatirkan, terbukti dari laporan yang dirilis oleh Otoritas Jasa Keuangan (OJK) yang menyatakan dari Januari 2020 hingga Maret 2021 terdapat 15.098 kasus terkait penagihan pinjaman online dengan melakukan pengungkapan data pribadi yang merusak kredibilitas, reputasi, dan/atau karakter nasabah. Kasus tersebut dapat dikategorikan sebagai jenis kejahatan siber doxing berupa delegitimasi. Bahkan unit pengaduan kejahatan siber Polri (Cyber Patrol), hingga September 2021 telah menerima 7 laporan kejahatan siber doxing berupa denominasi dan penargetan.

METODE

Metode penelitian yang digunakan adalah metode yuridis normatif dengan pendekatan perundang-undangan, pendekatan konseptual, pendekatan kasus.

HASIL DAN PEMBAHASAN

A. Realita Kejahatan Siber di Indonesia

Perkembangan teknologi internet dengan jejaring sosialnya telah membentuk suatu masyarakat baru dalam wujud virtual. Masyarakat ini merupakan wajah lain dari masyarakat nyata yang disebut masyarakat siber (cybercommunity/cybersociety). Bentuk masyarakat ini berada pada ruang virtual, di mana tidak dibutuhkan kehadiran fisik dari anggotamasyarakatnya. Suatu ruang yang tidak lagi mempersoalkan sekat-sekat antar bangsa, yang menjadikanya sebagai desa global. Berbagai proses sosial terjadi seperti bercinta, menyapa, bergaul, berbisnis, dan belajar. Perkembangan cybercommunity ini menjadi simbol kemajuan peradaban manusia. Dengan teknologi ini, segala aktivitas manusia dimudahkan.1

Selain memberikan kemaslahatan bagi kehidupan manusia, dampak penemuan ini juga berpengaruh terhadap sisi gelap kehidupan manusia. Masalah-masalah sosial dalam dunia nyata juga turut merambah ke dalam

dunia virtual ini. Perilaku-perilaku kejahatan dalam cybercommunity yang biasa disebut cybercrime turut meramaikan dinamika kehidupan di dalamnya. Kalau dalam dunia nyata dikenal tindakan kriminalitas pencurian dan perampokan Bank, sedangkan di dalam cybercommunity juga ditemukan kasus kriminalitas serupa seperti pembobolan rekening lewat fasilitas internet Banking.

Maraknya cybercrime yang terjadi di dalam cybercommunity, menunjukan gejala pergeseran masalah sosial dari dunia nyata. Sifat cybercommunity yang tanpa batas teritorial dan tanpa kendali, di mana tindak kejahatan sulit untuk dilacak, dan telah

[1] Anto, Rusdi. 2018. *Kasus-Kasus Cyber Crime sebagai Dampak Perkembangan Teknologi Komunikasi yang Meresahkan Masyarakat*. Pusat Studi Perencanaan dan Pembangunan Masyarakat, Jakarta, hlm.1-3.

menjadi ruang yang ideal untuk berkembangnya masalah-masalah sosial. Tindak kejahatan ini dalam prateknya menggunakan teknologi telematika canggih yang sulit untuk dilihat dan dapat dilakukan dimana saja, sehingga potensi untuk berkembangnya masalah sosial menjadi sulit untuk dihentikan.2

B. Kesiapan Regulasi dan Kebijakan dalam Mengantisipasi dan Mengatasi Kejahatan Siber Doxing di Indonesia

Bahwa ancaman kejahatan siber, khususnya kejahatan siber doxing di Negara Republik Indonesia menunjukan prevalensi yang terus berkembang dari waktu ke waktu, sehingga penyelenggara negara dipandang perlu untuk memberikan perhatian khusus, terutama dari aspek pengaturan regulasi.

Diketahui, bahwa sebelum disahkannya Undang-Undang ITE dan Undang-Undang PDP, tindak pidana siber doxing bisa dipidanakan dengan menggunakan Undang-Undang Hukum Pidana, pasal 362, tentang Pencurian, yang berbunyi:

"Barang siapa mengambil barang sesuatu, yang seluruhnya atau sebagian kepunyaan orang lain, dengan maksud untuk dimiliki secara melawan hukum, diancam karena pencurian, dengan pidana penjara paling lama lima tahun atau pidana denda paling banyak sembilan ratus rupiah".

Namun, narasi yang sampaikan pada pasal tersebut tidak spesifik menyentuh hal-hal yang berkaitan dengan pencurian data secara elektronik. Hal inilah salah satu alasan yang kemudian mendorong pemerintah untuk membuat dan mensahkan UU ITE.3 Namun demikian, instrumen tersebut dipandang belum sepenuhnya mengatur secara khusus, tentang hal-hal yang menyangkut kejahatan siber, Pemerintah dalam membentuk UU ITE ini masih menggunakan pendekatan politis pragmatis, bukan menggunakan pendekatan kebijakan publik yang melibatkan lebih banyak kalangan. UU ITE lebih banyak mencermati transaksi elektronik yang dipakai dalam dunia bisnis, meski siapa pun tahu bahwa dunia siber (cyberspace) lebih luas dari sekedar transaksi elektronik. Termasuk ketentuan-ketentuan yang menyangkut tentang pelaksanaan perbuatan jahat atau perbuatan yang dapat dihukum dalam UU ITE, misalnya pada tindakan kelalaian atau khilaf.

Kebijakan kriminalisasi tindak pidana siber di Indonesia yang ideal adalah dibentuknya Undang-Undang Khusus tentang Tindak Pidana Siber. Dalam Undang-Undang Khusus ini dirumuskan aturan umum yang akan berlaku untuk semua tindak pidana di bidang teknologi informasi dan komunikasi, tindak pidana yang berkaitan dengan kerahasiaan, keutuhan, dan ketersediaan data atau sistem komputer/sistem elektronik, pedoman pemidanaan, hukum acara yang mengatur prosedur penyelidikan dan penyidikan di bidang teknologi informasi dan komunikasi, termasuk penggeledahan dan penyitaan alat bukti digital, kerja sama internasional seperti ekstradisi, bantuan hukum timbal balik, dan kerja sama internasional lainya dalam penyelidikan dan

[2] *Ibid*

[3] Petrus Reinhart Gollose. 2006. *Perkembangan Cyber Crime Dan Upaya Penanganannya Di Indonesia Oleh Polri*. Buletin Hukum Perbankan, Jilid/Vol.4, No.2, hlm.19.

penyidikan tindak pidana siber.4

Pada tanggal 17 Oktober 2022, Pemerintah telah menetapkan Undang- Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). UU PDP tersebut merupakan lex specialis dan dapat dianggap sebagai nomenklatur tindak pidana kejahatan siber khusus yang terkait dengan "data pribadi".

Problematika Regulasi Kejahatan Siber di Indonesia

Meski UU ITE telah mengatur jenis-jenis perbuatan yang dapat dikriminalisasi sebagai tindak pidana, penambahan jenis alat bukti baru, dan imunisasi eksistensi alat bukti elektronik, namun masih terdapat permasalahan hukum dalam penanganan tindak pidana siber di Indonesia, yaitu:[5]

1. Permasalahan dalam menentukan tempat terjadinya tindak pidana (locus delicti) dan waktu kejadian tindak pidana (tempus delicti). Dalam tindak pidana siber, penyidik sering mengalami kesulitan dalam menentukan lokasi atau tempat yang akurat terjadinya tindak pidana. Karena pelaku dapat menghapus atau mengubah "jejak digital" perangkat yang dipergunakannya untuk melakukan tindak pidana siber maupun mengubah data lokasi yang berbeda. Begitu pun halnya dengan dalam menentukan waktu kejadian perkara. Penyidik memiliki kesulitan dalam menentukan secara pasti kapan terjadinya perbuatan tersebut karena umumnya pelaku ini memiliki kemampuan untuk mengubah atau mengacaukan waktu dan tanggal perbuatannya dilakukan
2. Permasalahan barang bukti juga menjadi problematik tersendiri bagi aparat penegak hukum. Barang bukti yang dicari adalah terkait dengan segala sesuatu yang dipergunakan untuk mempersiapkan, untuk melakukan, dan hasil tindak pidana siber sangat sulit untuk melacaknya karena dibalik kecanggihan sistem jaringan internet juga memiliki celah bagi orang-orang yang memiliki keahlian untuk menghapus atau memalsukan identitasnya di dunia maya. Di sisi lain, teknologi informasi adalah teknologi dengan sistem yang terbuka yang tidak mustahil untuk dapat dibajak atau diduplikasi (cloning) secara ilegal, di mana setiap orang yang memiliki keahlian di bidang tersebut dapat memanipulasi data, mengubah data, seperti menjadikan data palsu (fake data) menjadi data yang asli atau sebaliknya.
3. Tindak pidana siber ini dapat memiliki karakteristik dilakukan oleh satu orang dalam ruangan tertutup, sehingga untuk beberapa bentuk tindak pidana siber biasa, penyidik sulit untuk mendapatkan saksi yang menyaksikan langsung pelaku saat sedang melakukan tindak pidana siber, sehingga saksi yang dimiliki terbatas pada saksi korban. Dalamhal tindak pidana siber terkait dengan perbankan, bisa saja pihak perbankan cenderung menutupi telah terjadinya serangan tindak pidana siber terhadap mereka, karena hal ini menjadi aib yang dapat menghilangkan kepercayaan masyarakat secara umum dan nasabah penyimpan dana di bank tersebut.

[4] Wahyu Beny Mukti Setiyawan, Erifendi Churniawan; Femmy Silaswaty Faried. 2020. *Upaya Regulasi Teknologi Informasi Dalam Menghadapi Serangan Siber Guna Menjaga Kedaulatan Negara Kesatuan Republik Indonesia*. Jurnal USM Law Review, Jilid/Vol.3, No.2, hlm.282-284.

[5] *Ibid.*, hlm.287-288.

4. Pada Pasal 37 UU ITE disebutkan: "Setiap Orang dengan sengaja melakukan perbuatan yang dilarang sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 36 di luar wilayah Indonesia terhadap Sistem Elektronik yang berada di wilayah yurisdiksi Indonesia."

Meski telah jelas dinyatakan bahwa yurisdiksi UU ITE juga melingkupi perbuatan "dari luar" wilayah yurisdiksi Indonesia, tetapi yurisdiksi suatu negara yang diakui hukum internasional dalam pengertian konvensional, didasarkan pada batas-batas geografis, sementara kejahatan siber dapat bersifat internasional, multi yurisdiksi, dan tanpa batas, sehingga sampai saat ini belum dapat dipastikan bagaimana yurisdiksi suatu negara dapat diberlakukan terhadap kejahatan siber dengan pemanfaatan teknologi dan jaringan informasi. Dengan demikian terkait kewenangan hukum/yurisdiksi dalam penindakannya juga dapat menimbulkan permasalahan yang serius, hal ini dikarenakan internet tidak mengenal batas wilayah. Sehingga sangat mungkin saja terjadi tarik menarik kewenangan oleh beberapa negara yang merasa dirugikan oleh tindak pidana siber dalam penegakan hukumnya.

Pelaksanaan atau pemberlakuan hukum tindak pidana nasional suatu negara erat kaitannya dengan tempat terjadinya tindak pidana (*locus delicti*). *Locus delicti* menjadi suatu problematika hukum apabila pelaku tindak pidana dan penyelesaian tindak pidana tidak berada dalam satu tempat yang sama, tetapi di dua atau lebih tempat yang berbeda. Dalam tindak pidana siber, tindakan atau perbuatan dapat dilakukan dimanapun karena dilakukan dengan komputer dengan internet dan/atau sistem jaringannya serta dapat menimbulkan akibat yang bersifat lintas batas.[6]

KESIMPULAN

1. Realita kejahatan siber khususnya kejahatan siber doxing di Indonesia tampak menjadi suatu permasalahan sosial yang berimplikasi terhadap timbulnya permasalahan hukum. Hal ini ditandai dengan banyaknya bermunculan kasus kejahatan siber, khususnya kejahatan siber doxing di masyarakat. Salah satu timbulnya permasalahan ini di antaranya dipengaruhi oleh perkembangan teknologi yang berkembang sangat cepat dan masif, dimana keadaan tersebut harus dilihat terlebih dahulu dari induk kejahatan siber yaitu ruang maya (cyberspace) yang merupakan sebuah realitas baru dalam kehidupan manusia, diawali dengan: (a) terjadinya perubahan-perubahan dalam masyarakat sebagai akibat adanya perkembangan inovasi teknologi, (b) inovasi tersebut menjadi cara alternatif seseorang berinteraksi sebagai mahkluk sosial, pola interaksi sosial baru ini memunculkan suatu bentuk masyarakat baru dalam wujud virtual yaitu masyarakat siber (cybercommunity/ cybersociety), (d) maraknya kejahatan siber yang terjadi di dalam masyarakat siber menunjukkan adanya pergeseran problematika sosial dari dunia nyata, (e) saat ini muncul bentuk kejahatan siber baru bernama doxing yang khusus terjadi di lingkungan dan masyarakat siber berupa pelanggaran hak atas data pribadi. Kondisi ini pada gilirannya menimbulkan permasalahan sosial di masyarakat,

[6] Setiyawan, Churniawan, Faried, *Op.Cit.*, hlm.291

yaitu munculnya kecemasan, kekhawatiran, dan rasa takut akan terjadinya ancaman hilangnya harta, benda serta harkat dan martabat, baik individu maupun kelompok masyarakat, sehingga perlu dilakukan langkah-langkah konkret dari penyelenggara negara, khususnya yang membidangi tugas penegakan hukum.

2. Kesiapan regulasi dalam mengantisipasi dan mengatasi kejahatan siber khususnya kejahatan siber doxing di Indonesia, pada hakikatnya sudah dan terus dilakukan dengan disahkannya dan dikeluarkannya 2 (dua) instrumen penting, antara lain yaitu; Undang-Undang Informasi dan Transaksi Elektronik serta Undang-Undang Perlindungan Data Pribadi. Namun demikian, kedua instrumen tersebut faktanya belum sepenuhnya dapat memberi jaminan kepastian hukum, yang ditandai dengan kurang terakomodirnya proses penegakan hukum terhadap kejahatan siber, khususnya kejahatan siber doxing. Berkenaan dengan hal tersebut, maka lembaga legislatif dipandang perlu untuk melakukan berbagai pendekatan yang dapat mendorong lahirnya produk hukum terkait pengaturan kejahatan siber doxing. Pendekatan tersebut antara lain diawali dengan melakukan: (a) analisis regulasi umum atas tindak kejahatan siber, (b) analisis regulasi khusus atas tindak kejahatan siber, dan (c) analisis problematika regulasi kejahatan siber khususnya kejahatan siber doxing.

DAFTAR PUSTAKA

Literatur Buku:

Anto, Rusdi. 2018. Kasus-Kasus Cyber Crime sebagai Dampak Perkembangan Teknologi Komunikasi yang Meresahkan Masyarakat. Pusat Studi Perencanaan dan Pembangunan Masyarakat, Jakarta, hlm.1-3.

Wahid, Abdul dan Labib, Mohammad. 2005. Kejahatan Mayantara (Cybercrime). Refika Aditama, Bandung.

Widodo. 2009. Sistem Pemidanaan Dalam Cyber Crime Alternatif Ancaman Pidana Kerja Sosial Dan Pidana Pengawasan Bagi Pelaku Cyber Crime. Laksbang Mediatama, Yogyakarta

Jurnal :

Petrus Reinhart Gollose. 2006. Perkembangan Cyber Crime Dan Upaya Penanganannya Di Indonesia Oleh Polri. Buletin Hukum Perbankan, Jilid/Vol.4, No.2, hlm.19.

Wahyu Beny Mukti Setiyawan, Erifendi Churniawan; Femmy Silaswaty Faried. 2020. Upaya Regulasi Teknologi Informasi Dalam Menghadapi Serangan Siber Guna Menjaga Kedaulatan Negara Kesatuan Republik Indonesia. Jurnal USM Law Review, Jilid/Vol.3, No.2, hlm.282-284.