

DELIK-DELIK DILUAR KUHP (TINDAK PIDANA CYBER CRIME DAN CARA PENANGGULANGAN)

Rozi Yudha Febriansyah

Fakultas Hukum Universitas 17 Agustus 1945 Surabaya

Abstrak

Perkembangan teknologi khususnya di bidang telekomunikasi dan transportasi dianggap sebagai lokomotif dan turut mempercepat proses globalisasi di berbagai aspek kehidupan. Perkembangan yang sangat pesat dari teknologi telekomunikasi dan komputer menghasilkan internet yang multifungsi. Dengan perkembangan teknologi ini membuat globe dunia seolah-olah menjadi seperti hanya selebar daun kelor. Perkembangan ini juga membawa perubahan yang besar dan mendasar pada tatanan sosial dan budaya pada skala global. Namun di balik kemudahan layanan inter itu terdapat ancaman dari sisi keamanannya. Teknologi informasi yang menghasilkan internet memiliki dampak yang positif namun juga memiliki dampak yang negatif. Internet adalah jaringan global yang dapat digunakan untuk berkomunikasi dari satu lokasi satu ke lokasi lainnya dibelahan dunia seperti sekolah, universitas, riset, museum, bank, perusahaan bisnis, perorangan, stasiun TV ataupun radio. Hal yang harus diperhatikan adalah keamanan sistem informasi berbasis internet perlu diperhatikan, karena jaringan internet yang bersifat publik dan global sangat rentan dari berbagai kejahatan. Ancaman tersebut timbul apabila seseorang berkeinginan memperoleh akses ilegal dalam jaringan komputer, merusak jaringan, mencuri data dengan memanfaatkan teknologi internet yang canggih untuk melakukan kejahatan yang dapat merugikan orang lain. Kejahatan ini di kenal dengan kejahatan dunia maya atau cyber crime.

Kata kunci: delik-delik, tindak pidana, cyber crime

Latar Belakang

Perkembangan teknologi khususnya di bidang telekomunikasi dan transportasi dianggap sebagai lokomotif dan turut mempercepat proses globalisasi di berbagai aspek kehidupan. Perkembangan yang sangat pesat dari teknologi telekomunikasi dan komputer menghasilkan internet yang multifungsi. Dengan perkembangan teknologi ini membuat globe dunia seolah-olah menjadi seperti hanya selebar daun kelor.

Perkembangan ini juga membawa perubahan yang besar dan mendasar pada tatanan sosial dan budaya pada skala global. Namun di balik kemudahan layanan inter itu terdapat ancaman dari sisi keamanannya. Teknologi informasi yang menghasilkan internet memiliki dampak yang positif namun juga memiliki dampak yang negatif. Internet adalah jaringan global yang dapat digunakan untuk berkomunikasi dari satu lokasi satu ke lokasi lainnya dibelahan dunia seperti sekolah, universitas, riset, museum, bank, perusahaan bisnis, perorangan, stasiun TV ataupun radio. (Gumilang et al., 2019)

Hal yang harus diperhatikan adalah keamanan sistem informasi berbasis internet perlu diperhatikan, karena jaringan internet yang bersifat publik dan global sangat rentan dari berbagai kejahatan. Ancaman tersebut timbul apabila seseorang berkeinginan memperoleh akses ilegal dalam jaringan komputer, merusak jaringan, mencuri data dengan memanfaatkan teknologi internet yang canggih untuk melakukan kejahatan yang dapat merugikan orang lain. Kejahatan ini di kenal dengan kejahatan dunia maya atau cyber crime. (Tomy Michael, n.d.)

Saat ini kebutuhan adanya internet didominasi para kalangan pelajar mulai dari sekolah dasar (SD) sampai dengan SMU dan Mahasiswa, Dewasa bahkan sampai orang tua. Kehadiran internet memang seperti pisau bermata dua, disatu sisi teknologi ini bisa bermanfaat apabila digunakan untuk melakukan hal-hal yang baik dan bermanfaat seperti : mencari bahan materi pelajaran sekolah, diskusi pelajaran, mencari program beasiswa, belajar jarak jauh. Sedangkan dampak negatifnya adalah banyak situs-situs pornografi, pornoaksi, perjudian, kekerasan dan lain-lain, yang

mengakibatkan maraknya tindakan-tindakan perkosaan, pelecehan seksual yaitu gemar membuka situs-situs terlarang di internet, selain itu maraknya tindakan-tindakan dunia maya seperti carding, hacking, membobol password orang lain, facebook, twitter, instagram, yang merupakan situs jejaring pertemanan. Penculikan para remaja melalui facebook, yang merupakan situs jaringan pertemanan sampai pada kasus yang menyangkut musisi JRX versus IDI Bali yaitu pencemaran nama baik yang dilakukan JRX kepada IDI Bali, dari contoh tersebut dapat dilihat bahwa globalisasi teknologi juga dibarengi oleh globalisasi kejahatan. (Kleden, 2019)

Fenomena kejahatan cyber crimes sendiri di Indonesia semakin lama semakin meningkat dengan berbagai kasus yang bervariasi seperti kasus pemakaian nama domain Mustika Ratu. com, YKCI vs Indosat (Royalti 'ring back tone'), Kasus lain adalah perusakan fasilitas internet banking BCA dengan membuat situs tiruan www.klikbca.com oleh seorang hacker seperti kilkbca.com, www.klickbca.com, klickbca.com, clickbca.com, Contoh lain pernah terjadi di beberapa kota besar seperti di Yogyakarta, Bandung, Semarang yaitu dengan ditangkapnya beberapa pemuda yang melakukan kejahatan cyber crime dengan modus carding (kejahatan internet dengan membobol kartu kredit orang lain untuk bertransaksi) yang membuat Indonesia menjadi salah satu Negara terkenal dalam cybercrime dan modus hacking (perusakan jaringan komputer pihak lain). Kasus yang menghebohkan lagi adalah hacker bernama Dani Hermansyah, pada tanggal 17 April 2004 melakukan deface dengan mengubah nama-nama partai yang ada dengan nama-nama buah dalam website www.kpu.go.id yang mengakibatkan berkurangnya kepercayaan masyarakat terhadap pemilu yang sedang berlangsung pada saat itu. (Saputra & Mahyani, 2017) Di kota Surakarta sendiri kasus cybercrime belum pernah mencuat, akan tetapi yang terbaru adalah adanya kasus pembobolan data melalui email yang dilakukan warga pasarkliwon.

Dalam penggunaannya sendiri salah satu contoh situs di internet yaitu facebook bisa dikatakan dapat memberikan dampak positif dan negatif bagi seseorang. Dampak positif yang dirasakan oleh para pengguna facebook selain untuk sarana bersosialisasi, komunikasi, rekreasi, chatting, berkomunikasi dengan teman lama, facebook pun berfungsi untuk sarana berdiskusi bahkan sampai bisa digunakan untuk mengumpulkan bantuan untuk kegiatan sosial seperti koin untuk prita, koin untuk bilqis dsb. Sedangkan dampak negative dari penggunaan facebook yaitu membuat orang menjadi malas belajar, hanya membuang-buang waktu bahkan memicu adanya tindak kejahatan berupa penipuan, pelecehan, sampai terjadinya penculikan dan para korban penculikan rata-rata dialami oleh perempuan yang kebanyakan masih berstatus sebagai pelajar. Budaya global tersebut secara positif memiliki muatan ilmu pengetahuan, teknologi, politik, sosial dan kebudayaan, tetapi juga memiliki dampak negative manakala disalahgunakan. Ancaman atau bahaya yang datang dari internet bagi anak-anak dan remaja menjadi perhatian serius bagi masyarakat Indonesia. Dalam makalah ini, penulis membahas tentang penanggulangan kejahatan internet di Indonesia. (Cahyono & Wahyono, 2017) Masyarakat khususnya para remaja yang sekarang sedang digandrungi oleh situs-situs di internet dan paham betul tentang penggunaan internet, perlu dibekali berbagai informasi, dalam rangka untuk mengetahui tentang dampak negatif perkembangan teknologi informasi seperti internet dan tentang penanggulangan kejahatan cybercrime dari aspek hukum, maka diberikan penyuluhan dan pengertian seputar dampak dari perkembangan teknologi informasi, kemudian peraturan yang berkaitan dengan perkembangan teknologi informasi seperti UU ITE No 11 Tahun 2008 yang didalamnya mengatur tentang perbuatan-perbuatan yang dilarang yang berkaitan dengan pencurian, penipuan, perjudian, pencemaran nama baik dst.

Rumusan Masalah

1. Jelaskan apa yang dimaksud cyber crime
2. Bagaimana cara mencegah cyber crime agar tidak merajalela

Tujuan Penelitian

1. Untuk mengetahui apa yang di maksud cyber crime
2. Untuk mengetahui cara agar cyber crime tidak semakin merajalela

Metode Penelitian

Mencari kebenaran secara ilmiah atau spesifik tentang tindak pidana cyber crime serta menanggulangi tindak pidana cyber crime. (Michael, n.d.)

Pembahasan

Cyber crime atau kejahatan dunia maya adalah kejahatan yang dilakukan oleh seseorang maupun kelompok yang menguasai dan mampu mengoperasikan komputer dan alat telekomunikasi lainnya. Cara-cara yang biasa yang dilakukan dengan merusak data, mencuri data dan menggunakannya secara ilegal. Menurut Abdul Wahib dan Mohammad Labib, cyber crime merupakan salah satu jenis kejahatan yang membahayakan individu, masyarakat dan negara. Jenis kejahatan ini (cyber crime) tidak tepat jika disebut sebagai 'crime without victim', tetapi dapat dikategorikan sebagai kejahatan yang dapat menimbulkan korban berlapis-lapis baik secara privat maupun publik. (Suhartono, 2020) Hak privat dapat terancam, terganggu, bahkan rusak atau hilang akibat ulah segelintir orang atau beberapa orang yang memanfaatkan kelebihan ilmu yang dimiliki dan teknologi dengan modus operandi yang tergolong dalam cyber crime.

Indra Safitri mengatakan bahwa cybercrime sebagai kejahatan dunia maya

yaitu jenis kejahatan yang berkaitan dengan pemanfaatan sebuah teknologi informasi tanpa batas serta memiliki karakteristik yang kuat dengan sebuah rekayasa teknologi yang mengandalkan kepada tingkat keamanan yang tinggi dan kredibilitas dari sebuah informasi yang disampaikan dan diakses oleh pelanggan internet.

John Spiropoulos mengatakan bahwa cybercrime memiliki sifat efisien dan cepat serta sangat menyulitkan bagi pihak penyidik dalam melakukan penangkapan terhadap pelakunya.

Cyber crime yang menggunakan media komunikasi dan komputer, meskipun berada di dunia maya tetapi memiliki dampak yang sangat nyata. Penyimpangan dan kerugian besar telah terjadi dan berdampak luas kepada sektor-sektor ekonomi, perbankan, moneter, budaya bahkan dapat mengancam pertahanan dan keamanan negara. Agar tidak dikucilkan dalam pergaulan global, Indonesia harus mengantisipasi dan melakukan langkah konkrit dalam penanggulangan kejahatan internet.

Kualifikasi kejahatan dunia maya (cyber crime), sebagaimana dikutip Barda Nawawi Arief, adalah kualifikasi cybercrime menurut Convention on Cybercrime 2001 di Budapest Hongaria, yaitu: (1) Illegal access: yaitu sengaja memasuki atau mengakses sistem komputer tanpa hak; (2) Illegal interception: yaitu sengaja dan tanpa hak mendengar atau menangkap secara diam-diam pengiriman dan pemancaran data komputer yang tidak bersifat publik ke, dari atau di dalam sistem komputer dengan menggunakan alat bantu teknis; (3) Data interference: yaitu sengaja dan tanpa hak melakukan perusakan, penghapusan, perubahan atau penghapusan data computer; (4) System interference: yaitu sengaja melakukan gangguan atau rintangan serius tanpa hak terhadap fungsinya sistem computer; (5) Misuse of Devices: penyalahgunaan perlengkapan komputer, termasuk program komputer, password komputer, kode masuk (access code); (6) Computer related Forgery: Pemalsuan (dengan sengaja dan tanpa hak memasukkan, mengubah, menghapus data

otentik menjadi tidak autentik dengan maksud digunakan sebagai data autentik); (7) Computer related Fraud: Penipuan (dengan sengaja dan tanpa hak menyebabkan hilangnya barang/kekayaan orang lain dengan cara memasukkan, mengubah, menghapus data computer atau dengan mengganggu berfungsinya komputer/sistem computer, dengan tujuan untuk memperoleh keuntungan ekonomi bagi dirinya sendiri atau orang lain).

Mencegah Cyber Crime

Untuk mencegah merajalelanya tindakan yang termasuk kategori cyber crime, pemerintah bersama aparaturnya perlu segera melakukan tindakan-tindakan penanggulangan dan penegakan hukum yaitu dengan mensosialisasikan, merealisasikan dan mengimplementasikan berbagai peraturan dan perundang-undangan yang telah ada seperti dalam KUHP dan UU ITE untuk menjerat para pelaku kejahatan cyber crime. (Wahyono et al., 2020) Sebelum munculnya UU ITE No 11 Tahun 2008, untuk menjerat pelaku cyber crime, dipakai undang-undang yang bersifat khusus dan ketentuan-ketentuan yang bersifat umum, seperti: Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi; Undang-Undang Nomor 5 Tahun 1999 tentang Larangan Praktek Monopoli dan Persaingan Usaha yang Tidak Sehat, Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen, Undang-Undang Nomor 19 Tahun 2002 tentang Hak Cipta, Undang-Undang Nomor 14 Tahun 2001 tentang Hak Paten; Undang-Undang Nomor 15 Tahun 2001 tentang Merk, dan KUHP. Dalam prakteknya, yang sering dipakai adalah Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi dan KUHP.

UU Nomor 20 Tahun 2001 jo UU Nomor 31 Tahun 1999 tentang Tindak Pidana Pemberantasan Korupsi yaitu dengan memasukkan alat bukti elektronik sebagai alat bukti yang sah, dalam bentuk 'petunjuk', yang diatur dalam Pasal 26 A yang menyatakan sebagai berikut: "Alat bukti yang sah dalam bentuk petunjuk sebagaimana dimaksud dalam Pasal 188 ayat (2) Undang-undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana, khusus untuk tindak pidana korupsi juga dapat diperoleh dari: Alat bukti yang berupa informasi yang diucapkan, dikirim, diterima, atau disimpan secara elektronik dengan alat optik atau yang serupa dengan itu; dan Dokumen. Para pelaku cyber crime dikenakan pasal-pasal dalam KUHP seperti penipuan, pengrusakan server KPU, penggelapan dan pasal pidana lain diluar KUHP seperti UU telekomunikasi dan UU lain yang memiliki sangsi pidana. Untuk KUHP yang sering digunakan adalah: (1) Pasal 362 KUHP dapat dikenakan untuk kasus carding dimana pelaku mencuri nomor kartu kredit milik orang lain. (2) Pasal 378 KUHP dapat dikenakan untuk penipuan dengan seolah-olah menawarkan dan menjual suatu produk atau barang dengan memasang iklan, tetapi, pada kenyataannya ,barang tersebut tidak ada. Hal tersebut dike-tahui setelah uang dikirimkan dan barang yang dipesan tidak datang sehingga pembeli tersebut merasa tertipu. (3) Pasal 335 KUHP dapat dikenakan untuk kasus pengancaman dan pemerasan yang dilakukan melalui e-mail yang dikirimkan oleh pelaku untuk memaksa korban melakukan sesuatu sesuai dengan apa yang diinginkan oleh pelaku dan jika tidak dilaksanakan akan membawa dampak yang membahayakan. Hal ini biasanya dilakukan karena pelaku biasanya mengetahui rahasia korban. (4) Pasal 311 KUHP dapat dikenakan untuk kasus pencemaran nama baik dengan menggunakan media Internet. Modusnya adalah pelaku menyebarkan e-mail kepada teman-teman korban tentang suatu cerita yang tidak benar atau mengirimkan e-mail kesuatu mailing list sehingga banyak orang mengetahui cerita tidak benar tersebut. (5) Pasal 303 KUHP dapat dikenakan untuk menjerat permainan judi yang dilakukan secara online di Internet dengan penyelenggara dari Indonesia. (6) Pasal 282 KUHP dapat dikenakan untuk penyebaran pornografi maupun website porno yang banyak beredar dan mudah diakses di Internet. Walaupun berbahasa

Indonesia, sangat sulit sekali untuk menindak pelakunya karena mereka melakukan pendaftaran domain tersebut di luar negeri dimana pornografi yang menampilkan orang dewasa bukan merupakan hal yang ilegal. (8) Pasal 406 KUHP dapat dikenakan pada kasus deface atau hacking yang membuat system milik orang lain, seperti website atau program menjadi tidak berfungsi atau dapat digunakan sebagaimana mestinya. Dalam UU ITE beberapa pasal-pasal yang penting adalah:(Hidayat et al., 2020) (1) Pasal 30 ayat (1) yang menyebutkan: "Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik milik orang lain dengan cara apapun, dipidana dengan pidana penjara paling lama 12 tahun / denda paling banyak Rp. 600 Juta. (2) Pasal 46, ayat (2) "Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik dengan cara apapun dengan tujuan untuk memperoleh informasi elektronik dan/atau dokumen elektronik, dipidana dengan pidana penjara paling lama 7 tahun dan / denda paling banyak Rp. 700 Juta. Sedangkan ayat (3) "Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/ atau sistem elektronik dengan cara apapun dengan melanggar, menerobos, melampaui atau menjebol sistem pengamanan, dipidana dengan pidana penjara paling lama 8 tahun dan / atau denda paling banyak Rp. 800 Juta. (3) Kemudian Pasal 31 sampai dengan pasal 37. Gugatan kelompok atau biasa dikenal dengan class action, dinaungi oleh Pasal 38 ayat 2. Di dalam UU tersebut juga dinyatakan bahwa masyarakat dapat mengajukan gugatan perwakilan terhadap pihak yang menyelenggarakan sistem elektronik yang berakibat merugikan masyarakat.

Penanggulangan Cyber Crime Di Indonesia

Pengamanan Software Jaringan Komputer; Tindakan preventif yg dapat dilakukan dalam rangka pengamanan software jaringan komputer sbb:(Angraeni & Nasution, 2019) (1) Mengatur akses (access control), melalui mekanisme authentication dengan menggunakan password. (2) Firewall, program yang merupakan sebuah perangkat yang diletakkan antara internet dengan jaringan internal yang berfungsi untuk menjaga agar akses ke dalam maupun keluar dari orang yang tidak berwenang tidak dapat dilakukan. (3) Intruder Detection System (IDS), diantaranya adalah Autbase, mendeteksi probing dengan memonitor log file. (4) Backup rutin, untuk cadangan manakala sistem kita berhasil dimasuki pihak lain. (intruder) dll. Langkah-langkah yang dapat dilakukan adalah: Penguncian computer, Penggunaan dial back, adalah penggunaan telepon double, antara telepon kirim dengan telepon terima, dengan cara bergantian dalam pemakaian saluran telepon. Salah satu persoalan yang muncul terkait dengan perkembangan kejahatan transnasional adalah penegakkan hukumnya terhadap para pelaku cyber crime. Kejahatan transnasional dalam cyber crime jelas akan bersinggungan dengan masalah yurisdiksi. Dalam ruang siber pelaku pelanggaran sulit untuk ditindak oleh karena pelakunya berada di luar wilayah Indonesia. Hal inilah yang kemudian menjadi persoalan yurisdiksi dari penegakan cybercrime di Indonesia. Artinya hukum mana yang akan diberlakukan dalam menangani kejahatan cybercrime tersebut.

Aspek Instrumen Hukum

Agar penegakkan hukum dapat terlaksana dengan baik maka harus dipenuhi empat syarat, yaitu: (1) Adanya aturan perundang-undangan khusus mengatur dunia cyber. (2) Adanya lembaga yang akan menjalankan peraturan yaitu polisi, jaksa dan hakim khusus yang khusus menangani cyber crime. (3) Adanya fasilitas atau sarana untuk mendukung pelaksanaan peraturan itu. (4) Kesadaran hukum dari masyarakat yang terkena peraturan. Tujuan pembentukan undang-undang yang khusus mengatur tentang dunia maya ini adalah untuk pemberatan atas tindakan pelaku agar

dapat menimbulkan efek jera dan mengatur sifat khusus dari sistem pembuktian. Dengan adanya undang-undang yang khusus mengatur cybercrime maka dapat mempermudah bagi aparat penegak hukum dalam penegakan hukum.

Aspek Aparatur Penegak Hukum

Penegak hukum di Indonesia mengalami kesulitan dalam menghadapi merebaknya cybercrime, beberapa penyebab diantaranya adalah keterbatasan Sumber Daya Manusia yang dimiliki penegak hukum, yakni sangat langka yang intens terhadap kejahatan komputer, kejahatan yang menggunakan sarana komputer, kejahatan dunia maya. Sebab kejahatan ini memerlukan ketrampilan khusus bagi aparaturnya. Sehingga dalam hal penyelidikan dan penyidikan selalu mengalami jalan buntu atau tidak tuntas. Metode penyidikannya juga bersifat khusus, tidak semua penyidik dapat melakukannya. Harus ada anggota kepolisian yang bertugas di bidang internet atau biasa disebut polisi cyber atau cyber police.

Untuk membuktikan jejak-jejak para hacker, cracker dan phreaker dalam melakukan aksinya terutama yang berhubungan dengan program-program dan data-data komputer, sarana Polri belum memadai karena belum ada komputer forensik. (Setyorini et al., 2020) Fasilitas ini diperlukan untuk mengungkap data-data digital serta merekam dan menyimpan bukti-bukti berupa soft copy (image, program, dsb). Dalam hal ini Polri masih belum mempunyai fasilitas forensic computing yang memadai. Fasilitas forensic computing yang akandirikan Polri diharapkan akan dapat melayani tiga hal penting yaitu evidence collection, forensic analysis, expert witness. Aplikasi di lapangan menunjukkan bahwa pelaku cybercrime dikenakan dengan pasal-pasal dalam KUHP seperti penipuan, pengrusakan, penggelapan dan pasal pidana lain diluar KUHP seperti undang-undang telekomunikasi, undang-undang hak cipta dan yang terbaru adalah undang-undang ITE.

Kesimpulan

Kejahatan di dunia cyberyang tidak lagi mengenal batas-batas suatu Negara sehingga menimbulkan persoalan-persoalan baru dan dampaknya telah dirasakan oleh masyarakat pengguna computer dan jaringannya. Oleh karena itu selain sudah adanya pengaturan hukum juga diperlukan strategi penanggulangan cyber crime. Penanggulangan dimaksud dimulai dari upaya pencegahan kejahatan cyber crime yaitu pendekatan secara teknologi dengan pengamanan software, hardware, kemudian dilakukan upaya sosialisasi computer dan internet di tengah-tengah masyarakat, pendekatan kultur juga bisa dilakukan dengan cara menerapkan etika. Dalam rangka mewujudkan penegakan hukum terhadap kejahatan Cyber crime harus didukung tiga aspek yang terkait dengan penegakan hukum yaitu aspek instrumen hukum, aparat penegak hukum dan aplikasinya di lapangan. Aspek Instrumen adalah dengan adanya berbagai undang-undang termasuk UU ITE yang dapat meminimalisir dan dapat dijadikan payung hukum terhadap penindakan kejahatan cybercrime.

Peran orangtua juga berperan penting untuk melakukan pengawasan agar anak-anak terhindar dari tindak kejahatan cyber crime dan juga anak-anak tidak menjadi pelaku baru dalam kejahatan cyber crime

Daftar Pustaka

- Angraeni, K. D., & Nasution, K. (2019). KEKUATAN HUKUM LoU SEBAGAI JAMINAN DALAM KREDIT SINDIKASI BANK. *Jurnal Hukum Bisnis Bonum Commune*.
<https://doi.org/10.30996/jhbbc.v2i2.2521>
- Cahyono, D. J. P., & Wahyono, D. (2017). PENYELESAIAN PERSELISIHAN ANTARA BADAN PENYELENGGARA PERGURUAN TINGGI SWASTA DENGAN DOSEN. *Mimbar Keadilan*.

<https://doi.org/10.30996/mk.v0i0.2198>

- Gumilang, D., Yudianto, O., & Setyorini, E. H. (2019). LEGALITAS SURAT KUASA YANG DITERBITKAN SEORANG BURON. *Jurnal Hukum Magnum Opus*.
<https://doi.org/10.30996/jhmo.v2i2.2497>
- Hidayat, M. R., Nasution, K., & Setyadji, S. (2020). Kekuatan Hukum Pengikat Hak Tanggungan Atas Jaminan Kredit. *Jurnal Akrab Juara*. <https://doi.org/10.11693/hyhz20181000233>
- Kleden, K. L. (2019). PENDEKATAN VIKTIMOLOGI MEMINIMALISIR DISPARITAS PIDANA. *Jurnal Hukum Magnum Opus*. <https://doi.org/10.30996/jhmo.v2i2.2611>
- Michael, T. (n.d.). PEMBERDAYAAN MAHASISWA DALAM MENUMBUHKAN JIWA MENULIS ILMIAH MELALUI PELATIHAN ARTIKEL DI FAKULTAS HUKUM UNIVERSITAS 17 AGUSTUS 1945 SURABAYA. *Jurnal Akrab Juara*, 5(1), 66–72.
- Saputra, A., & Mahyani, A. (2017). TINJAUAN YURIDIS TRADING IN INFLUENCE DALAM TINDAK PIDANA KORUPSI. *Mimbar Keadilan*. <https://doi.org/10.30996/mk.v0i0.2201>
- Setyorini, E. H., Sumiati, S., & Utomo, P. (2020). KONSEP KEADILAN RESTORATIF BAGI ANAK YANG BERKONFLIK DENGAN HUKUM DALAM SISTEM PERADILAN PIDANA ANAK. *DiH: Jurnal Ilmu Hukum*. <https://doi.org/10.30996/dih.v16i2.3255>
- Suhartono, S. (2020). HUKUM POSITIF PROBLEMATIK PENERAPAN DAN SOLUSI TEORITIKNYA. *DiH: Jurnal Ilmu Hukum*, 15(2), 206.
- Tomy Michael, W. L. S. (n.d.). Holiday Overview In Indonesia General Election (Is That Legal?). *Opcion Revista Activa*, 35(30), 389–400.
- Wahyono, D., Suseno, I., Aziz, K., & Sukendar, A. Y. S. (2020). *Validity for Ownership of the Floating Houses on the Coast*. <https://doi.org/10.2991/aebmr.k.200226.041>