

Kebijakan Hukum Pidana dalam Mengimplementasikan, Nilai Keadilan, dan Kepastian Hukum dalam Ruang Lingkup *Cyber Law*

Abimayu Prana Sakti. Fakultas Hukum, Universitas Pasundan, Mayuchanel25@gmail.com

ABSTRACT: With the advancement of computer technology integrated with the cyber world, various cybercrimes have emerged that require specific regulations. Cybercrimes frequently occurring in Indonesia include fraud through email, e-banking, and e-commerce. The Indonesian government responded by enacting the ITE Law No. 11 of 2008 to prosecute perpetrators of cybercrimes. This research uses a literature review method by collecting data from various sources such as books, journals, newspapers, and literature. The study examines the definitions of cyber law and cybercrime, causal factors, and steps to combat cybercrime. In the discussion, it was found that public legal awareness and modernization of national criminal law are key factors in addressing cybercrimes. In addition, law enforcement against cybercrimes requires international cooperation and adjusting regulations to global standards. This research emphasizes the importance of increasing public legal awareness and the role of law enforcement agencies that understand information technology. Efforts in socialization and education to the public are crucial steps in reducing cybercrimes. Thus, it is hoped that comprehensive criminal law policies can create justice and legal certainty in the cyber world.

KEYWORDS: Cyber Law, Cybercrime, Justice, Legal Certainty, ITE Law, Law Enforcement.

ABSTRAK: Dengan kemajuan teknologi komputer yang terintegrasi dengan dunia cyber, muncul berbagai kejahatan siber atau *cybercrime* yang memerlukan regulasi khusus. *Cybercrime* yang sering terjadi di Indonesia termasuk penipuan melalui email, ebanking, dan *e-commerce*. Pemerintah Indonesia merespons dengan mengesahkan “Undang-Undang ITE No. 11 Tahun 2008” untuk menjerat pelaku kejahatan dunia maya. Penelitian ini menggunakan metode studi pustaka dengan mengumpulkan data dari berbagai sumber seperti buku, jurnal, surat kabar, dan literatur. Studi ini mengkaji definisi *cyber law* dan *cybercrime*, faktor penyebab, serta langkah-langkah penanggulangan *cybercrime*. Dalam pembahasan, ditemukan bahwa kesadaran hukum masyarakat dan modernisasi hukum pidana nasional merupakan faktor kunci dalam menghadapi kejahatan siber. Selain itu, penegakan hukum terhadap *cybercrime* memerlukan kerja sama internasional dan penyesuaian regulasi dengan standar global. Penelitian ini menekankan pentingnya peningkatan kesadaran hukum masyarakat serta peran aparat penegak hukum yang memahami teknologi informasi. Upaya sosialisasi dan edukasi kepada masyarakat menjadi langkah

penting dalam mengurangi kejahatan siber. Dengan demikian, diharapkan bahwa kebijakan hukum pidana yang komprehensif dapat menciptakan keadilan dan kepastian hukum dalam dunia *cyber*.

KATA KUNCI: *Cyber Law*, *Cybercrime*, Keadilan, Kepastian Hukum, Undang-Undang ITE, Penegakan Hukum.

I. PENDAHULUAN

Di milenium ketiga ini, yang ditandai dengan era teknologi informasi, kita diperkenalkan dengan dunia maya (*cyberspace*) dan internet yang memungkinkan komunikasi tanpa kertas (*paperless document*) (Ersya, 2017). Saat ini, integrasi teknologi informasi yang merata dalam kehidupan sehari-hari kita tidak dapat disangkal, berdampak langsung maupun tidak langsung pada kita.

Secara khusus, kemajuan dalam teknologi komputer dan internet memiliki implikasi signifikan terhadap regulasi dan pembentukan hukum cyber serta terhadap perkembangan kejahatan dalam dunia maya. Kejahatan mayantara (*cybercrime*), yang lahir dari kemajuan teknologi yang cepat, telah menjadi perhatian utama di tingkat internasional. Penjahat mayantara memanfaatkan kemajuan teknologi untuk melakukan kejahatan yang berdampak negatif pada berbagai aspek masyarakat modern (Djura, 2023).

Meningkatnya kasus kejahatan mayantara, terutama di Indonesia, mendorong pemerintah untuk mengesahkan Undang-Undang yang mampu mengadili para pelaku kejahatan di dunia maya. Pemerintah Indonesia telah mengesahkan Undang-Undang *Cybercrime* sebagai bagian dari "UU ITE No. 11 tahun 2008", yang bertujuan untuk mengatasi, meminimalisir, dan membuat jera terhadap kegiatan kejahatan mayantara. Namun, aparat penegak hukum menghadapi tantangan dalam melacak para pelaku kejahatan mayantara karena sifat kejahatan yang dinamis.

Menurut pakar teknologi Roy Suryo, "Kejahatan mayantara marak terjadi di lima kota besar di Indonesia, yang dilakukan oleh para hacker, kebanyakan adalah individu muda yang terlihat kreatif tetapi sebenarnya melakukan kegiatan seperti mencuri nomor kartu kredit secara online" (Aldriano & Priyambodo, 2022).

Cybercrime dapat dibagi menjadi dua jenis: definisi sempit dan luas. Secara sempit, melibatkan kejahatan terhadap sistem komputer,

sedangkan secara luas, mencakup kejahatan terhadap sistem komputer, jaringan, dan kejahatan yang dimungkinkan oleh penggunaan computer.

Andi Hamzah (1989) mendefinisikan *cybercrime* sebagai setiap aktivitas kriminal yang melibatkan komputer, umumnya merujuk pada penggunaan ilegal komputer. *Cybercrime* memanfaatkan teknologi komputer, khususnya internet, sebagai alat utama untuk kegiatan kriminal (Indah dkk, 2021).

Menurut survei MarkPlus *Insight Netizen*, jumlah pengguna internet di Indonesia mencapai 61 juta pada tahun 2012, atau sekitar 23,5% dari populasi, dengan 40% dari mereka menghabiskan lebih dari 3 jam online setiap hari. Lebih lanjut, 58 juta orang mengakses internet menggunakan perangkat mobile seperti telepon dan tablet. Indonesia menempati peringkat kedelapan secara global dalam jumlah pengguna internet, dan proyeksi menunjukkan peningkatan signifikan dalam penggunaan internet hingga tahun 2015 dibandingkan dengan tahun 2010 (Boston Consulting Group) (Setiawan dkk, 2013).

II. METODE

Metode pendekatan yang diterapkan adalah yuridis normatif, yang mengkaji norma-norma hukum yang terdapat dalam peraturan perundang-undangan, doktrin hukum, serta putusan pengadilan yang terkait dengan *cybercrime*. Sumber data penelitian mencakup data primer dari peraturan perundang-undangan seperti “Undang-Undang ITE No. 11 Tahun 2008”, dan data sekunder dari literatur hukum, jurnal ilmiah, serta putusan pengadilan. Pengumpulan data dilakukan melalui studi dokumen terhadap peraturan perundang-undangan, doktrin hukum, dan putusan pengadilan terkait. Analisis data dilakukan secara deskriptif analitis, yang bertujuan untuk menjelaskan norma hukum yang ada dan menganalisis penerapannya dalam konteks kejahatan siber.

III. HASIL PENELITIAN & PEMBAHASAN

A. Definisi *Cyber Law* dan *Cyber Crime*

Cyber Law mencakup segala aspek hukum yang terkait dengan individu atau subjek hukum yang menggunakan serta memanfaatkan teknologi internet, yang dimulai saat mereka masuk ke dalam dunia maya atau *cyber*. Istilah ini berasal dari "*cyberspace law*" dan digunakan secara internasional untuk merujuk pada hukum yang terkait dengan penggunaan teknologi informasi. Istilah lain yang sering digunakan termasuk Hukum Teknologi Informasi (*Law of Information Technology*), Hukum Dunia Maya (*Virtual World Law*), dan Hukum Mayantara.

Cybercrime, atau kejahatan siber, merupakan bentuk-bentuk kejahatan yang muncul karena pemanfaatan teknologi internet. Beberapa pendapat menganggap *cybercrime* setara dengan kejahatan komputer. Departemen Kehakiman Amerika Serikat mendefinisikan kejahatan komputer sebagai: "setiap tindakan ilegal yang membutuhkan pengetahuan tentang teknologi komputer untuk pelaksanaannya, penyelidikan, atau penuntutannya." Definisi ini sejalan dengan Organisasi Pengembangan Komunitas Eropa yang mendefinisikan kejahatan komputer sebagai: "setiap perilaku ilegal, tidak etis, atau tidak sah yang berkaitan dengan pengolahan otomatis dan/atau transmisi data." Andi Hamzah (1989), dalam tulisannya "Aspek-aspek Pidana di Bidang Komputer," mengartikan kejahatan komputer sebagai: "penggunaan komputer secara illegal (Ketaren, 2016).

Cybercrime dapat didefinisikan sebagai kejahatan yang melanggar hukum dengan menggunakan teknologi komputer sebagai alat pelakunya, dimungkinkan oleh kemajuan teknologi informasi terutama internet. Tingkat kejahatan di dunia maya tergantung pada pengetahuan dan kesadaran pengguna serta sumber daya seperti hardware dan software yang mereka miliki terkait keamanan *cyber*. Para penyedia layanan atau target *cybercrime* harus memahami metode yang biasanya digunakan oleh pelaku kejahatan ini.

Ruang lingkup *Cyber Law* mencakup berbagai aspek, seperti *Hate Speech* (ucapan kebencian), *Trademark* (merek dagang), *Defamation* (pencemaran nama baik), *Copyright* (hak cipta), *Privacy* (privasi), *Duty Care* (kewajiban kehati-hatian), *Criminal Liability* (pertanggungjawaban pidana), *Hacking*, *Viruses*, *Illegal Access* (akses ilegal), *Regulation Internet Resource* (pengaturan sumber daya internet), *Procedural Issues* (masalah prosedural seperti yurisdiksi, pembuktian, penyelidikan), *Pornography* (pornografi), *Robbery* (pencurian), *Electronic Contract* (kontrak elektronik), *E-Commerce* (perdagangan elektronik), *E-Government* (pemerintahan elektronik), dan *Consumer Protection* (perlindungan konsumen) (Rohmy & Suratman, 2021).

Cybercrime dapat dibedakan berdasarkan motifnya menjadi dua kategori:

1. *Cybercrime* sebagai kejahatan murni adalah tindakan kriminal di mana seseorang dengan sengaja dan terencana melakukan perusakan, pencurian, atau tindakan anarkis terhadap suatu sistem informasi atau komputer.
2. *Cybercrime* sebagai kejahatan abu-abu adalah tindakan kriminal yang tidak jelas statusnya sebagai kejahatan kriminal atau bukan karena meskipun terjadi pembobolan, tetapi tidak ada perusakan, pencurian, atau tindakan anarkis terhadap sistem informasi atau komputer tersebut (Akub, 2018).

Beberapa faktor yang menyebabkan kejahatan komputer (*Cybercrime*) adalah:

1. Ketersediaan akses internet yang luas memungkinkan jaringan saling terhubung sehingga mempermudah pelaku kejahatan untuk melakukan tindakan kriminal.
2. Kesalahan atau kelalaian dari pengguna komputer juga dapat memfasilitasi terjadinya *cybercrime*.

3. Meskipun kejahatan komputer dapat dilakukan dengan mudah dan tanpa peralatan yang canggih, risiko keamanannya relatif kecil. Namun, pelacakan pelaku kejahatan menjadi sulit, sehingga mendorong mereka untuk terus melakukan aktivitas tersebut.
4. Pelaku *cybercrime* seringkali memiliki kecerdasan yang tinggi, memiliki rasa ingin tahu yang besar terhadap teknologi komputer, dan biasanya memiliki pengetahuan yang mendalam tentang cara kerja komputer, melebihi pengetahuan seorang pengguna komputer biasa.
5. Kurangnya perhatian dari masyarakat dan penegak hukum terhadap masalah keamanan *cyber* juga dapat memfasilitasi terjadinya *cybercrime*.
6. Kelemahan dalam sistem keamanan jaringan juga menjadi faktor pendukung terjadinya *cybercrime*.
7. *Cybercrime* dipandang sebagai kegiatan yang menghasilkan keuntungan ekonomi bagi para pelakunya.

Contoh Kasus *Cyber Crime* yang ada di Indonesia

1. Pada tahun 2008, di Indonesia, kasus pornografi yang sangat mencuat adalah kasus Ariel-Luna-Cut Tari. Kasus ini melibatkan aksi mempublikasikan video porno Ariel "PeterPan" bersama Luna Maya dan Cut Tari di internet oleh seseorang dengan inisial 'RJ'. Saat ini, kasus ini masih menjadi perbincangan luas, dengan penyerangan tersebut ditujukan kepada individu yang memiliki karakteristik tertentu sesuai dengan tujuan penyerangan. Penanganan kasus ini dilakukan melalui proses hukum, dimana pengunggah video dan individu terlibat dalam video tersebut dijerat dengan "Pasal 29 Undang-Undang Republik Indonesia Nomor 44 Tahun 2008 tentang Pornografi Pasal 56". Ancaman hukumannya minimal enam bulan hingga 12 tahun penjara, atau denda minimal Rp 250 juta hingga Rp 6 miliar, dan/atau "Pasal 282 ayat 1 Kitab Undang-Undang Hukum Pidana".

2. Prita Mulyasari digugat dan dilaporkan ke polisi oleh Rumah Sakit Omni Internasional karena dituduh melakukan pencemaran nama baik melalui surel. Kasus ini dimulai dari surel yang ditulis oleh Prita yang mengisahkan pengalamannya saat dirawat di unit gawat darurat Rumah Sakit Omni Internasional. Prita Mulyasari dijerat dengan “Pasal 27 Undang-Undang Informasi dan Transaksi Elektronik (UU ITE)”, dengan ancaman hukuman maksimal 6 tahun penjara dan denda sebesar Rp 1 miliar (Ketaren, 2016).

B. Penanggulangan *Cybercrime* dan Pengaturan Hukumnya

Studi kriminologi mengenai kejahatan di dunia maya menunjukkan perkembangan yang signifikan. Meskipun berbagai upaya pencegahan dan penanggulangan telah dilakukan, namun kejahatan mayantara atau kejahatan dunia maya terus mengalami penyebaran yang luas. Penegak hukum menjadi pihak utama yang harus berperan aktif dalam memerangi *cybercrime*. Contohnya, Resolusi PBB Nomor 5 tahun 1963 mengenai upaya penanggulangan penyalahgunaan Teknologi Informasi pada tanggal 4 Desember 2001 menegaskan bahwa masalah ini merupakan isu internasional serius yang harus segera diatasi.

Di Indonesia, “Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE)” adalah undang-undang pertama yang secara khusus mengatur tindak pidana di ranah siber. Naskah UU ITE disampaikan secara resmi kepada DPR RI berdasarkan Surat Presiden RI No. R. /70/Pres/9/2005 tanggal 5 September 2005, dan disahkan pada tanggal 21 April 2008.

Meskipun UU ITE telah ada, realitasnya menunjukkan bahwa dunia siber tetap sulit untuk dikendalikan karena sifatnya yang virtual namun diakses oleh jutaan pengguna di seluruh dunia. Karakteristik ini menyebabkan UU ITE menghadapi kendala dalam penerapannya, terutama karena kejahatan siber sering kali lintas negara, yang menghadirkan tantangan terkait yurisdiksi atas tindak pidana dan pelakunya. Indonesia menyadari bahwa keterbatasan perundang-

undangan konvensional menjadi hambatan dalam menangani masalah ini, sehingga penyesuaian hukum diperlukan untuk menjaga kedaulatan dan kepentingan negara serta warganya (Setiawan dkk, 2013).

Untuk mengatasi penyebaran kejahatan internet (*Cybercrime*) yang semakin meluas, setiap negara perlu menyadari bahaya dari penyalahgunaan internet. Berikut adalah beberapa langkah atau cara penanggulangan secara global:

1. Modernisasi hukum pidana nasional serta prosedur hukumnya untuk disesuaikan dengan konvensi internasional yang berkaitan dengan kejahatan di dunia maya.
2. Peningkatan standar keamanan sistem jaringan komputer nasional agar sesuai dengan standar internasional.
3. Meningkatkan pemahaman dan keahlian aparat hukum dalam upaya pencegahan, penyelidikan, dan penuntutan kasus-kasus yang terkait dengan *cybercrime*.
4. Meningkatkan kesadaran masyarakat akan bahaya *cybercrime* dan pentingnya langkah-langkah pencegahan terhadap kejahatan tersebut.
5. Memperkuat kerja sama antarnegara dalam hal teknologi hukum terkait pelanggaran *cybercrime*.

Secara keseluruhan, penanggulangan *cybercrime* secara global membutuhkan kerja sama antarnegara dan penerapan standar undang-undang internasional yang konsisten (Ketaren, 2016).

Adapun pengaturan *cybercrime* mengacu pada sumber hukum yang berlaku baik dalam KUHP maupun undang-undang lainnya. Aturan hukum bentuk *cybercrime* di dalam KUHP dapat dilihat pada pasal-pasal berikut:

- a. “Pasal 362 KUHP tentang pencurian”;
- b. “Pasal 369 KUHP tentang Pemerasan dan Pengancaman”;

- c. “Pasal 372 KUHP tentang Penggelapan”;
- d. “Pasal 386 KUHP tentang Perbuatan Curang”;
- e. “Pasal 506 KUHP tentang Pelanggaran Ketertiban Umum”;
- f. “Pasal 382 bis KUHP”;
- g. “Pasal 383 KUHP”.

Pengaturan ini yang telah di himbau oleh PBB bahwa Negara untuk menanggulangi *cybercrime* dengan sarana penal (kebijakan hukum pidana yang menggunakan sanksi pidana sebagai cara menanggulangi kejahatan). Meskipun tantangannya besar, namun karena meningkatnya kasus *cybercrime* yang menimbulkan kekhawatiran di kalangan masyarakat, terutama bagi pengguna komputer dan informasi, maka perlindungan hukum bagi para korban adalah suatu kebutuhan yang mendesak untuk segera diimplementasikan oleh negara (Akub, 2018). Usaha penanggulangan kejahatan dengan hukum pidana pada hakikatnya merupakan bagian dari usaha penegakan hukum (Indah dkk, 2021).

C. Kesadaran Hukum Masyarakat

Walaupun telah ada Undang-Undang yang mengatur kejahatan di dunia maya, secara keseluruhan masih belum mampu mengendalikan perilaku masyarakat dalam memanfaatkan fasilitas dunia maya (Mastur, t.t.)

Kesadaran hukum masyarakat sangat penting dalam penegakan hukum *cyber law*. Kesadaran hukum masyarakat berperan sebagai salah satu faktor kunci dalam mengantisipasi dan mengatasi kejahatan *cyber*. Dalam konteks ini, kesadaran hukum masyarakat berarti bahwa masyarakat memiliki pengetahuan dan pemahaman yang baik tentang hukum *cyber law* dan cara-cara menghindari kejahatan *cyber*. Upaya meningkatkan kesadaran hukum masyarakat dapat dilakukan melalui berbagai cara, seperti:

1. Sosialisasi: Kegiatan sosialisasi tentang hukum *cyber law* dan cara-cara menghindari kejahatan *cyber* dapat membantu meningkatkan kesadaran masyarakat. Contohnya, kegiatan sosialisasi yang dilakukan oleh Tim PKBH FH UMY di Dukuh Jaten, Kelurahan Sendangadi, Kecamatan Mlati, Kabupaten Sleman, D.I Yogyakarta, membahas materi tentang kesadaran Masyarakat terkait, tingkat kesadaran masyarakat terkait hukum, penyebab pelanggaran hukum, penyebab ketaatan hukum, dan upaya untuk meningkatkan kesadaran hukum masyarakat.
2. Edukasi: Edukasi tentang keamanan *cyber* dan hukum *cyber law* dapat membantu meningkatkan kesadaran masyarakat. Penelitian menunjukkan bahwa kurangnya edukasi tentang kesadaran *cyber security* membuat banyak pengguna menjadi korban kejahatan siber. Oleh karena itu, edukasi tentang keamanan *cyber* dan hukum *cyber law* sangat penting untuk meningkatkan kesadaran masyarakat.
3. Pengembangan Hukum *Cyber Law*: Pengembangan hukum *cyber law* yang lebih efektif dan efisien dalam mengatasi kejahatan *cyber* juga sangat penting. Contohnya, “Undang-Undang Informasi dan Transaksi Elektronik (UU ITE)” dikeluarkan sebagai upaya untuk mengatur tata kelola teknologi informasi dan elektronik di Indonesia. Kesadaran akan UU ITE sangat penting bagi masyarakat desa agar terhindar dari berbagai tindakan ilegal atau penyalahgunaan teknologi informasi yang dapat merugikan diri sendiri maupun orang lain.

Tingkat kesadaran masyarakat terhadap *cybercrime* dalam penggunaan teknologi dan media sosial menunjukkan bahwa edukasi mengenai dampak buruknya kejahatan *cybercrime* telah memberikan masukan agar masyarakat dapat menghindari hal tersebut. Tingkat kewaspadaan dan kesadaran masyarakat terhadap bahaya *cybercrime* relatif tinggi, dengan persentase rata-rata mencapai 81,5% untuk kategori penggunaan media sosial dan 78,5% untuk kesadaran akan bahaya *cybercrime* dalam konteks penggunaan media sosial. Meskipun kesadaran

masyarakat terhadap bahaya *cybercrime* sudah cukup baik, tetap diperlukan kewaspadaan yang lebih tinggi. Terutama bagi mereka yang memiliki pengetahuan IT yang mendalam, penting untuk terus memberikan edukasi atau sosialisasi kepada masyarakat awam yang belum memiliki tingkat kesadaran dan kewaspadaan yang memadai. Beberapa persen dari masyarakat masih belum sepenuhnya sadar akan bahaya *cybercrime*, sehingga perlu upaya terus-menerus untuk meningkatkan kesadaran mereka. Selain itu, penting juga untuk terus mengikuti perkembangan terbaru mengenai *cybercrime* agar dapat mengetahui tanggapan dan respons publik terhadap kejahatan tersebut serta strategi mereka dalam menghadapinya (Pudjiarti dkk., 2023).

IV. KESIMPULAN

Dari penelitian ini adalah bahwa kebijakan hukum pidana dalam mengimplementasikan nilai keadilan dan kepastian hukum dalam ruang lingkup *cyber law* di Indonesia masih memiliki beberapa masalah. Kebijakan hukum *cybercrime* yang diterapkan melalui “Undang-Undang ITE no 11 tahun 2008” diharapkan dapat mengatasi dan meminimalisir kejahatan di dunia maya. Namun, masih terdapat beberapa masalah, seperti kurangnya kontrol aparat penegak hukum dalam pelacakan pelaku tindak pidana. Penelitian ini juga membahas definisi *cyber law* dan *cybercrime*, serta faktor-faktor yang mempengaruhi penegakan hukum terhadap *cybercrime*. Faktor-faktor tersebut meliputi hukum, penegak hukum, sarana dan fasilitas, serta masyarakat. Penelitian ini juga menyoroti beberapa contoh kasus *cybercrime* di Indonesia.

Dalam penelitian ini, penulis berharap dapat memberikan kontribusi pada pengembangan kebijakan hukum yang lebih efektif dalam menghadapi kejahatan di dunia maya dan memastikan kepastian hukum bagi masyarakat.

UCAPAN TERIMA KASIH

Puji dan syukur kami panjatkan ke hadirat Tuhan Yang Maha Esa atas segala rahmat dan karunia-Nya sehingga penelitian ini dapat diselesaikan dengan baik. Penelitian ini tidak akan berhasil tanpa bantuan, bimbingan, dan dukungan dari berbagai pihak yang telah memberikan kontribusi berharga selama proses penyusunan.

DAFTAR REFERENSI

- Akub, M. S. (2018). PENGATURAN TINDAK PIDANA MAYANTARA (CYBER CRIME) DALAM SISTEM HUKUM INDONESIA (Vol. 20, Nomor 2). <https://circlednewssite>.
- Aldriano, M. A., & Priyambodo, M. A. (2022). CYBER CRIME DALAM SUDUT PANDANG HUKUM PIDANA. *Jurnal Kewarganegaraan*, 6(1).
- Djura, A. (2023). TINJAUAN HUKUM CYBERCRIME DALAM SISTEM HUKUM INDONESIA. Dalam *Jurnal Hukum EGALITAIRE* (Vol. 1, Nomor 1).
- Ersya, M. P. (2017). <title/>. *Journal of Moral and Civic Education*, 1(1), 50–62. <https://doi.org/10.24036/8851412020171112>
- Indah, U., & Sari, P. (t.t.). KEBIJAKAN PENEGAKAN HUKUM DALAM UPAYA PENANGANAN CYBER CRIME YANG DILAKUKAN OLEH VIRTUAL POLICE DI INDONESIA (Vol. 2). www.mustikaratu.com
- ketaren, eliesta. (2016). CYBERCRIME, CYBER SPACE, DAN CYBER LAW.
- Mastur, O. : (t.t.). IMPLEMENTASI UNDANG-UNDANG NOMOR 11 TAHUN 2008 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK SEBAGAI TINDAK PIDANA NON KONVENSIONAL.
- Pudjiarti, E., Faizah, S., & Hardani, S. (2023). Analisa Kesadaran Masyarakat Terhadap Bahaya Cybercrime Pada Penggunaan Teknologi dan Media Sosial. *BINA INSANI ICT JOURNAL*, 10(1), 24–37.
- Rohmy, A. M., & Suratman, T. (2021). UU ITE Dalam Perspektif Perkembangan Teknologi Informasi dan Komunikasi. *DAKWATUNA Jurnal Dakwah dan Komunikasi Islam*, 7(2).

Sari, M. (t.t.). CYBER CRIME DAN PENERAPAN CYBER LAW DALAM PEMBERANTASAN CYBER LAW DI INDONESIA.

Setiawan, R., & Arista, M. O. (2013). EFEKTIVITAS UNDANG-UNDANG INFORMASI DAN TRANSAKSI ELEKTRONIK DI INDONESIA DALAM ASPEK HUKUM PIDANA (Vol. 2, Nomor 2). Mei-Agustus.