



ISSN Print: 2085-2339

ISSN Online: 2654-7252

# Jurnal Surya Kencana Satu: Dinamika Masalah Hukum dan Keadilan

**Editorial Office:** Fakultas Hukum, Universitas Pamulang,  
Jalan Surya Kencana No. 1, Pamulang Barat, Tangerang Selatan 15417, Indonesia.  
Phone/ Fax: +6221-7412566  
E-mail: [dinamikahukum\\_fh@unpam.ac.id](mailto:dinamikahukum_fh@unpam.ac.id)  
Website: <http://openjournal.unpam.ac.id/index.php/sks>

## Analisis Kasus Cyber Crime Di Indonesia: Tantangan Penegakan Hukum Dalam Menghadapi Kasus Cyber Crime

Melani Azzahra<sup>a</sup>, Nurwati<sup>b</sup>, Teguh Rama Prasja<sup>c</sup>,  
M Rendi Aridhayandi<sup>d</sup>

<sup>a</sup>, Fakultas Hukum, Universitas Djuanda. E-mail: [melaniazzahra524@gmail.com](mailto:melaniazzahra524@gmail.com)

<sup>b,d</sup> Dosen Fakultas Hukum, Universitas Djuanda. E-mail: [nurwati@unida.ac.id](mailto:nurwati@unida.ac.id),  
[rendi.aridhayandi@unida.ac.id](mailto:rendi.aridhayandi@unida.ac.id)

<sup>c</sup> Dosen Fakultas Hukum, Universitas Islam Riau. E-mail: [teguhramaprasja@law.uir.ac.id](mailto:teguhramaprasja@law.uir.ac.id)

Article	Abstract
<p><i>Received: Mart 07,2025;</i> <i>Reviewed: Mart 12,2025;</i> <i>Accepted: Mart,14,2025;</i> <i>Published: Mart 25,2025</i></p>	<p>Perkembangan teknologi informasi dan internet telah membawa dampak besar di berbagai bidang kehidupan, memiliki banyak efek positif dan negatif yang tidak dapat diabaikan. Salah satu dampak negatif semakin mudahnya pelaku kejahatan melakukan tindakan kriminal cyber crime melalui dunia maya. Kejahatan teknologi informasi secara umum mengacu pada aktivitas kriminal yang melibatkan komputer atau jaringan komputer, tetapi juga mencakup aktivitas kriminal tradisional yang menggunakan komputer atau jaringan komputer sebagai alat untuk memfasilitasi atau meningkatkan efisiensi kejahatan. Tujuan penelitian ini adalah untuk mengkaji berbagai kasus cyber crime yang terjadi di Indonesia. Selain itu, membahas tantangan utama dalam penegakan hukum terkait dengan cyber crime di Indonesia. Metode penelitian ini menggunakan metodologi analisis deskriptif. Data dikumpulkan melalui studi literatur, tinjauan pustaka termasuk buku, artikel ilmiah, laporan penelitian, dan berita terkait kejahatan dunia maya di Indonesia. Hasil penelitian menunjukkan bahwa perkembangan teknologi digital telah membuka peluang bagi berbagai bentuk kejahatan dunia maya, terdapat tantangan-tantangan yang dihadapi dalam penegakan hukum kejahatan siber di Indonesia.</p> <p><b>Kata Kunci : Cyber Crime; Tantangan; Penegakan Hukum; Indonesia</b></p>

---

The development of information technology and the internet has had a significant impact on various aspects of life, with many positive and negative effects that cannot be ignored. One of the negative impacts is the increasing ease with which criminals can commit cyber crimes through the virtual world. Information technology crimes generally refer to criminal activities involving computers or computer networks, but also encompass traditional criminal activities that use computers or computer networks as tools to facilitate or enhance the efficiency of the crime. The purpose of this research is to examine various cases of cyber crime that occur in Indonesia. In addition, it discusses the main challenges in law enforcement related to cyber crime in Indonesia. This research method uses a descriptive analysis methodology. Data were collected through literature studies, including books, scientific articles, research reports, and news related to cybercrime in Indonesia. The research results show that the development of digital technology has opened up opportunities for various forms of cybercrime, and there are challenges faced in enforcing cybercrime laws in Indonesia.

***Keywords: Cyber Crime; Challenges; Law Enforcement; Indonesia***

---

## **PENDAHULUAN**

Perkembangan dan kemajuan teknologi informasi yang sangat pesat telah mengubah kehidupan manusia di berbagai bidang, termasuk Indonesia. Hal ini telah menyebabkan munculnya undang-undang baru, yang menghasilkan peraturan baru yang harus dipatuhi oleh semua lapisan masyarakat. Dalam memelihara dan memperkuat persatuan dan kesatuan bangsa berdasarkan peraturan perundang-undangan juga untuk kepentingan nasional, pemerintah perlu lebih mengembangkan penggunaan dan pemanfaatan teknologi informasi. Globalisasi yang pesat di Indonesia berdampak signifikan terhadap perkembangan teknologi. Perkembangan teknologi yang pesat membawa kemudahan bagi masyarakat di berbagai bidang kehidupan. Salah satu bidang di mana teknologi telah mengalami kemajuan pesat adalah komunikasi, yang menjadi perhatian utama masyarakat umum. Perkembangan teknologi di bidang komunikasi telah memudahkan orang untuk berkomunikasi dengan anggota keluarga yang tinggal jauh. Lebih jauh lagi, teknologi juga memiliki dampak besar pada masyarakat dalam hal ini, dan kita melihat tingkat peningkatan kemudahan tertentu di sektor ekonomi juga. (Madrim and Nurhidayat 2023)

Namun, Indonesia adalah salah satu negara berkembang yang memiliki kemajuan yang lambat dalam teknologi komunikasi modern. Indonesia tidak terlalu mementingkan pengembangan teknologi atau penguasaan strategis. Yang terjadi saat ini adalah transfer teknologi dari negara-negara maju tidak secara otomatis dilakukan, yang memerlukan waktu untuk negara berkembang seperti Indonesia untuk menyesuaikannya. Ini juga merupakan alasan utama maraknya kejahatan teknologi atau cyber crime. (Habibi and Liviani 2020)

Di era digitalisasi yang pesat, Indonesia menghadapi tantangan serius akibat maraknya kejahatan dunia teknologi. Ancaman-ancaman ini mencakup serangan terhadap infrastruktur perbankan, pencurian data, penipuan daring, dan transaksi ilegal di dunia maya. Kejahatan dunia maya atau cyber crime telah menjadi perhatian banyak negara, dampaknya dapat menyebabkan kerugian ekstrem terhadap masyarakat secara keseluruhan, mengancam keamanan dan stabilitas nasional, serta menimbulkan risiko serius terhadap pertumbuhan ekonomi negara. (Sosial 2024)

Oleh karena itu, upaya perlindungan masyarakat dan infrastruktur nasional dari ancaman kejahatan dunia maya menjadi sangat penting. Terdapat tantangan yang muncul saat menegakkan hukum kejahatan teknologi informasi cyber crime di Indonesia terutama yang berkaitan dengan pengaturan penggunaan internet. Penanganan tindak pidana seperti penipuan, perjudian, dan pornografi masih berlandaskan pada ketentuan Kitab Undang-Undang Hukum Pidana (KUHP). Namun, perkembangan teknologi informasi dan komunikasi telah mengubah cara kita berdagang, berbelanja, berinvestasi, dan berbisnis. Hal ini membuka peluang bagi kejahatan siber untuk berkembang biak dan menyebar.

## **PERMASALAHAN**

Berdasarkan pendahuluan diatas, maka penulis membahas yang pertama mengenai apa saja kasus cyber crime yang terjadi di Indonesia ? serta bagaimana tantangan penegakan hukum dalam menghadapi kasus cyber crime di Indonesia ?

## **METODOLOGI**

Penulis menggunakan metodologi penelitian analisis deskriptif. Penelitian ini mencakup metodologi analisis deskriptif. Data dikumpulkan melalui studi literatur, tinjauan pustaka termasuk buku, artikel ilmiah, laporan penelitian, dan berita terkait kejahatan dunia maya di Indonesia. Selain itu, melakukan analisis terhadap beberapa kasus kejahatan dunia maya yang terjadi di Indonesia dalam beberapa tahun terakhir. Data yang diperoleh akan dianalisis untuk mengidentifikasi tantangan penegakan hukum dan memberikan rekomendasi untuk meningkatkan efektivitas serta perbaikan

## **PEMBAHASAN**

### **Kasus cyber crime yang terjadi di Indonesia**

Seiring dengan kemajuan pesat dalam teknologi informasi dan komunikasi, kejahatan siber atau tindak pidana dunia maya menjadi masalah besar di Indonesia. Penanganan kejahatan siber di Indonesia melibatkan banyak aspek, mulai dari pengembangan peraturan hukum hingga penguatan penegakan hukum dan kerja sama lintas negara. Fakta bahwa kejahatan dunia maya telah menjadi ancaman besar bagi sektor keamanan non-tradisional ditunjukkan oleh kasus dan kondisi kejahatan dunia maya di Indonesia. Kejahatan dunia maya, juga dikenal sebagai kejahatan cyber, adalah salah satu yang paling umum di Indonesia. Keamanan dan kemampuan suatu negara untuk memahami ancaman dengan mengutamakan aspek militer untuk memerangi ancaman tersebut. Dalam hukum Indonesia, kejahatan dunia maya atau kejahatan cyber juga sering disebut sebagai tindak pidana yang berkaitan dengan teknologi informasi. Merupakan kejahatan yang berbeda dengan kejahatan-kejahatan pada umumnya. Dengan lahirnya revolusi teknologi informasi, kejahatan dunia maya muncul.

Jumlah kejahatan dunia maya pada tahun 2022 meningkat secara signifikan dibandingkan periode yang sama pada tahun 2021, menurut data e-MP Robinopsnal Bareskrim Polri. Faktanya, kejahatan internet meningkat 14 kali lipat. Antara 1 Januari dan 22 Desember 2022, polisi menyelidiki 8.831 kasus. Kasus-kasus ini dipantau oleh seluruh jajaran Bareskrim Polri dan kepolisian setempat tengah. Polda Metro Jaya menangani kasus kejahatan siber terbanyak, dengan 3.709 kasus. (Pusiknas Bareskrim Polri 2021)

Teknologi komunikasi memiliki dampak yang signifikan terhadap perubahan perilaku komunikasi manusia. Hal ini mempunyai keuntungan yaitu memudahkan komunikasi, tetapi juga dapat mempunyai kekurangan. Salah satunya adalah memudahkan "penjahat" melakukan kejahatan. Kemajuan teknologi telah memungkinkan penjahat dunia maya untuk mengeksploitasi korbannya. Jenis kejahatan dunia maya yang paling umum meliputi peretasan, cracking, carding, defacement, phreaking, dll. Kasus kejahatan teknologi atau cyber crime yang terjadi dan merugikan banyak pihak di Indonesia meliputi;

Serangan peretas terhadap Pusat Data Nasional (PDN). Kementerian Komunikasi dan Informatika (Kemenkominfo) selaku penyelenggara PDN menyebutkan serangan peretas terjadi

pada 20 Juni 2024 . Peretasan PDN terjadi melalui serangan siber oleh Brain Cipher menggunakan ransomware, perangkat lunak yang bertindak cepat seperti virus. Data yang disimpan di server PDN merupakan data penting pemerintah seperti Nomor Induk Kependudukan (NIK), Kartu Tanda Penduduk (KTP), nomor telepon seluler, dan sebagainya. Data Pribadi Sensitif Lainnya. Badan Siber dan Sandi Negara (BSSN) menyatakan serangan peretas tersebut terjadi akibat kelalaian dan buruknya pengelolaan sistem Kementerian Komunikasi dan Informatika yang tidak melakukan backup atau pencadangan terhadap data yang tersimpan di server PDN. Kurangnya persiapan pemerintah terhadap masalah peretasan yang berulang telah membahayakan informasi pribadi ribuan orang. Serangan ransomware meningkatkan kemungkinan kebocoran data PDN, gangguan sistem, dan kerugian ekonomi, juga bagi masyarakat secara keseluruhan pengelolaan data pribadi masyarakat yang dapat diperjual belikan secara bebas. (Ramdhan, Florina, and Permadi 2024)

Pencurian Data di Aplikasi Tokopedia, platform belanja daring Tokopedia menjadi korban pencurian data pengguna oleh peretas yang tidak bertanggung jawab. Platform identik dengan warna hijau, mencuri data penggunanya seperti nama, tempat lahir, tanggal lahir, email, nomor telepon, kata sandi, dan aktivitas transaksi. Pihak Tokopedia mampu merespons dengan cepat, mengubah kata sandi dan berhasil melindungi kata sandi dan informasi pembayaran pengguna. Hal ini dikarenakan kata sandi yang diamankan secara algoritma, sehingga memerlukan waktu yang lama bagi para peretas jahat untuk bisa meretasnya. Tapi saat itu, adanya data pribadi bocor pada dark web dan dijual, termasuk 91 juta data. (Fathur 2020)

Kebocoran data pribadi konsumen terjadi pada tahun 2021 Tjahjo Kumolo, Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi (PANRB), mengungkapkan penyesalan atas penyebaran data yang diduga berasal dari Badan Penyelenggara Jaminan Sosial (BPJS) Kesehatan. Menteri TK meminta Kementerian Komunikasi dan Informatika untuk menyelesaikan kebocoran data peserta BPJS Kesehatan secara menyeluruh, yang mungkin mencakup data (ASN). Kebocoran data memengaruhi data pribadi 279 juta orang, termasuk nama, nomor telepon, alamat, gaji, dan data kependudukan. Kebocoran data juga dapat berdampak pada data ASN. Untuk melakukan penyelidikan tersebut, BPJS Kesehatan bekerja sama dengan Telkom, Kementerian Komunikasi dan Informatika, dan Badan Siber Nasional dan Sandi Negara (BSSN). Kementerian Komunikasi dan Informatika juga meminta direksi BPJS Kesehatan segera memverifikasi dan menyelidiki kembali informasi yang bocor. (Maulida and Utomo 2023)

Lemahnya sistem keamanan merupakan penyebab utama pencurian data dan serangan cyber, Tidak ada sistem keamanan yang sempurna hal ini dapat disebabkan oleh berbagai faktor, termasuk kurangnya sumber daya, ketidaktahuan, dan kesalahan manusia. Peretas biasanya

adalah orang-orang terpelajar yang tidak berasal dari kelas bawah, memiliki setidaknya beberapa pendidikan formal, dan mampu mengoperasikan atau menggunakan PC. Para pelaku yang melakukan petasan juga merupakan orang-orang terpelajar, tidak terdidik secara teknis, produktif secara ekonomi dan dianggap sebagai bagian dari kelas sosial bawah. Selain itu, seiring berkembangnya teknologi, serangan siber menjadi semakin kompleks dan sulit dideteksi. Kejahatan siber juga merupakan masalah serius di Indonesia, selain kasus – kasus cyber crime tersebut kasus kejahatan siber yang umum di Indonesia meliputi malware, phishing, DDoS, cyberstalking, identitas palsu, cyberbullying, dan serangan terhadap infrastruktur. Penting untuk terus memperbarui sistem keamanan dan meningkatkan kesadaran di kalangan pengguna Internet tentang risiko kejahatan dunia maya. Selain itu, kerja sama antar negara juga penting dalam memerangi kejahatan dunia maya, yang sering kali melibatkan pelaku dari berbagai negara.

### **Tantangan Penegakan Hukum dalam menghadapi kasus cyber crime di Indonesia**

Munculnya teknologi digital di dunia informasi dan komunikasi mempengaruhi semua aspek kehidupan manusia. Perkembangan gaya hidup masyarakat sejalan dengan pertumbuhan dan penyebaran budaya, kebiasaan, dan pengetahuan baru, yang dapat digunakan untuk melakukan tindakan kriminal. Menurut JE Sahetapy, kejahatan adalah masalah manusia. Akibatnya, kejahatan selalu ada di mana ada manusia. (Kurniasih, Prasja, and Milandry 2022)

Oleh karena itu, kejahatan meningkat seiring kemajuan peradaban negara, dan penegakkan hukum yang efektif diperlukan. Penegakan hukum dilakukan secara sistematis oleh seluruh sistem kepolisian dan lembaga penegak hukum lainnya yang menegakkan ketentuan perundang-undangan untuk menjaga peraturan, mengadili kejahatan, dan menjatuhkan sanksi atas setiap pelanggaran atau kejahatan yang dilakukan oleh pelaku kejahatan. (Hidayat, Nurwati, and Suprijatna 2024)

Hukum akan selalu mengikat dengan masyarakat, Jika tidak ada hukum yang memiliki kekuatan memaksa, maka individu memiliki kebebasan untuk melakukan apa pun yang tidak diatur oleh hukum. Berdasarkan asas legalitas, perbuatan yang tidak diatur oleh hukum tidak bertentangan dengan hukum. Sebagai institusi sosial, bukan hanya sistem peraturan, juga cara masyarakat menjalankan fungsi-fungsi sosial, seperti mengatur perilaku dan kepentingan anggota masyarakat. (Junadi et al. 2021)

Sesuai dengan bunyi pasal dalam Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, Indonesia adalah negara hukum, merupakan gagasan dasar yang melatar belakangi dibentuknya Undang-Undang Informasi Transaksi Elektronik. Undang-undang ITE tidak hanya berfungsi sebagai pendekatan dalam pengembangan telekomunikasi, teknologi informasi, dan transaksi elektronik, tetapi juga, terutama, berfungsi sebagai standar yang dapat menjamin perlindungan hukum, kepastian hukum, dan keadilan bagi para pihak. Tujuannya adalah untuk

pihak yang terlibat dalam penyelenggaraan informasi dan transaksi elektronik (perorangan, pengguna, masyarakat, lembaga swadaya masyarakat, badan ekonomi, penyelenggara, otoritas pemerintah, dan lain-lain). Saat ini Indonesia telah memiliki undang-undang yang mengatur permasalahan terkait teknologi informasi, yaitu Undang-Undang No 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, yang dikenal sebagai UU ITE. Akan tetapi, undang-undang tersebut tidak sepenuhnya mencakup seluruh ruang lingkup dunia maya. UU ITE saat ini hanya mencakup masalah seperti konten ilegal, akses tidak sah, penyadapan ilegal, manipulasi data atau sistem, penggunaan perangkat secara tidak sah, dan penipuan computer. Namun, UU ITE belum memperhitungkan serangan siber yang dapat mengancam keamanan dan pertahanan nasional Indonesia. (Priyatno and Aridhayandi 2018)

Tidak hanya itu tantangan-tantangan teknologi yang dihadapi lembaga penegak hukum menggaris bawahi kebutuhan mendesak untuk menghadapi kasus serangan siber yang terjadi. Karena kejahatan dunia maya yang kompleks lembaga penegak hukum harus memiliki pengetahuan dan keahlian yang diperlukan untuk mengidentifikasi, melacak, dan memerangi penjahat dunia maya. Sifat kejahatan dunia maya yang transnasional menambah lapisan kompleksitas tambahan. Mengatasi tantangan ini memerlukan kerja sama internasional yang lebih intensif Konektivitas lintas batas memerlukan kerja sama bilateral dan multilateral, termasuk berbagi data, koordinasi penegakan hukum, dan harmonisasi peraturan. Akhirnya, tantangan utama penegakan hukum yang dihadapi, meliputi; (Ade Andre Nicodemus 2023)

Pertama, lemahnya penegakan hukum, masalah hukum di Indonesia dapat timbul karena berbagai faktor, termasuk sistem peradilan, sumber daya hukum, minimnya sumber daya manusia di lembaga penegak hukum dan minimnya sarana dan prasarana, hal ini dapat menjadi kendala dalam penegakan hukum di Indonesia. Penegakan hukum di Indonesia masih jauh dari kata memuaskan, hal ini disebabkan kurangnya aparat penegak hukum dan fasilitas yang tidak memadai menjadi kendala serius. Petugas penegak hukum sering kali tidak memiliki keahlian untuk menangani kasus terkait teknologi. Serta situasi diperburuk oleh terbatasnya kemungkinan untuk melakukan investigasi.

Rendahnya literasi digital di masyarakat merupakan salah satu tantangan terbesar yang sering diabaikan. Meskipun teknologi menjadi bagian integrall dari kehidupan sehari-hari, banyak orang masih tidak menyadari potensi risiko kejahatan dunia maya, sehingga mudah terjebak dalam perangkapnya. Pendidikan dan kesadaran publik adalah kunci utama untuk mencegah serangan siber serta melindungi informasi pribadi, dengan masyarakat yang lebih sadar akan bahaya serangan siber dapat meminimalkan potensi akibat kejahatan dunia maya.

Kurangnya koordinasi antar lembaga juga menimbulkan tantangan dalam menegakkan hukum kejahatan dunia maya. Kasus-kasus cyber crime sering kali melibatkan banyak lembaga,

namun koordinasi di antara lembaga-lembaga tersebut kurang optimal, sehingga berdampak pada efisiensi pemrosesan kasus. Mengatasi tantangan ini memerlukan solusi yang komprehensif dan terpadu. Salah satu cara untuk mencapai hal ini adalah dengan mengubah atau merevisi UU ITE untuk memperluas cakupan pengaturannya, menyesuaikannya dengan perkembangan teknologi, dan meminimalkan celah hukum yang dapat dimanfaatkan oleh penjahat dunia maya. Diharapkan melalui penguatan kolaborasi antar lembaga yang terlibat dalam penanganan kasus siber, Indonesia dapat menciptakan ruang digital yang aman dan bebas dari kejahatan daring serta meningkatkan penegakan hukum dan perlindungan korban. (Mei-et al.2024)

## PENUTUP

Kejahatan dunia maya di Indonesia menunjukkan bahwa perkembangan teknologi digital memungkinkan berbagai jenis kejahatan dunia maya, termasuk penipuan daring, peretasan, dan pencurian identitas. Meskipun Indonesia memiliki berbagai peraturan untuk memerangi kejahatan dunia maya, seperti Undang-Undang Informasi dan Transaksi Elektronik (ITE), penegakan hukum di bidang ini masih menghadapi tantangan besar. Tantangan utama yang dihadapi penegakan hukum kejahatan dunia maya di Indonesia meliputi kurangnya personel yang terlatih dalam bidang kejahatan dunia maya, terbatasnya infrastruktur untuk melacak dan memerangi kejahatan dunia maya yang semakin canggih, dan kurangnya koordinasi antara berbagai lembaga penegak hukum masalah seperti koordinasi antara keduanya. Selain itu, undang-undang yang ada masih belum secara memadai memperhitungkan perkembangan teknologi yang pesat, sehingga memungkinkan banyak penjahat dunia maya untuk mengeksploitasi celah hukum untuk menghindari hukuman. Untuk mengatasi masalah ini, diperlukannya kapasitas sumber daya manusia di bidang cyber dan memperbarui regulasi untuk beradaptasi dengan perkembangan teknologi. Selanjutnya, untuk mengembangkan sistem perlindungan yang lebih baik terhadap kejahatan dunia maya, pemerintah, sektor swasta, dan masyarakat harus bekerja sama lebih erat.

## DAFTAR PUSTAKA

- Fathur, Muhammad. 2020. "Tanggung Jawab Tokopedia Terhadap Kebocoran Data Pribadi Konsumen (Tokopedia's Responsibility for the Leakage of Consumers Personal Data)." *Procceding: Call for Paper 2nd National Conference on Law Studies: Legal Development Towards A Digital Society Era* 43–60.
- Habibi, Miftakhur Rokhman, and Isnatul Liviani. 2020. "Kejahatan Teknologi Informasi (Cyber Crime) Dan Penanggulangannya Dalam Sistem Hukum Indonesia." *Al-Qanun: Jurnal Pemikiran Dan Pembaharuan Hukum Islam* 23(2):400–426. doi: 10.15642/alqanun.2020.23.2.400-426.
- Hidayat, Husain Rahmat, Nurwati, and Dadang Suprijatna. 2024. "Peran Kepolisian Dalam Penanggulangan Tindak Pidana Perjudian Online Studi Kasus : Wilayah Kepolisian Resor Subang, Jawa Barat." *Karimah Tauhid* 3(3):3050–66. doi: 10.30997/karimahtauhid.v3i3.12481.
- Junadi, Yudi, Dedi Mulyadi, M. Rendi Aridhayandi, and Christopher Surya Salim. 2021. "Urgensi Pembatasan Periodisasi Masa Jabatan Anggota Legislatif Dalam Perspektif Konfigurasi Politik Hukum Indonesia." *Jurnal Hukum Mimbar Justitia* 7(2):140. doi: 10.35194/jhmj.v7i2.2043.



- Kurniasih, Esy, Teguh Rama Prasja, and Anggraini Dwi Milandry. 2022. "Perlindungan Konsumen Dalam Hal Pelaksanaan Tanggung Jawab Pengusaha Travel Tanpa Izin Operasional." *Jurnal Analisis Hukum* 5(2):231–44. doi: 10.38043/jah.v5i2.3741.
- Madrim, and Nurhidayat. 2023. "Perlindungan Hukum Terhadap Penyalahgunaan Data Pribadi Dalam Transaksi Pinjaman Online." *Journal Sains Student Research* 1(2):669–76. doi: 10.61722/jssr.v1i2.269.
- Maulida, One, and Hari Utomo. 2023. "Pertanggungjawaban Badan Penyelenggara Jaminan Sosial (BPJS) Kesehatan Atas Kebocoran Data Pribadi Pengguna Dalam Perspektif Hukum Pidana." *Indonesian Journal of Law and Justice* 1(2):10. doi: 10.47134/ijlj.v1i2.2011.
- Mei-, Djhpi, Alief Tanding Pamungkas, Andi Mulyono, and Nurjana Lahangatubun. 2024. "Krisis Penegakan Hukum Cybercrime Di Indonesia : Hambatan Dan Jalan Keluar The Crisis of Cybercrime Law Enforcement in Indonesia : Obstacles and Solutions."
- Priyatno, Dwidja, and M. Rendi Aridhayandi. 2018. "Resensi Buku (Book Review) Satjipto Rahardjo, Ilmu Hukum, Bandung: PT. Citra Aditya, 2014." *Jurnal Hukum Mimbar Justitia* 2(2):881. doi: 10.35194/jhmj.v2i2.36.
- Ramdhan, Tanzil Wahyu, Ike Desi Florina, and Didi Permadi. 2024. "Analisis Framing Pemberitaan Peretasan Pusat Data Nasional ( PDN) Di Media Online Tempo.Co." *Journal of Education Research* 5(3):3368–79. doi: 10.37985/jer.v5i3.1491.
- Sosial, Jurnal Ilmu. 2024. "Al-Dalil." 2(2).
- Nicodemus, Ade Andre. "Tantangan Dalam Penegakan Hukum Pidana Terhadap Kejahatan Siber Di Era Digital." Sekolah Tinggi Hukum IBLAM, 2023.
- Pusiknas Bareskrim Polri. "Kejahatan Siber Di Indonesia Naik Berkali-Kali Lipat." 2021[https://pusiknas.polri.go.id/detail\\_artikel/kejahatan\\_siber\\_di\\_indonesia\\_naik\\_berkali-kali\\_lipat](https://pusiknas.polri.go.id/detail_artikel/kejahatan_siber_di_indonesia_naik_berkali-kali_lipat), diakses pada tanggal 20 januari 2025.