QISTINA: Jurnal Multidisiplin Indonesia
Vol. 3 No. 2 Desember 2024
P-ISSN: 2964-6278 E-ISSN: 2964-1268

Efektivitas Hukum dan Kebijakan Publik dalam Menghadapi Ancaman Siber terhadap Keamanan Negara

Vannya Anastasya[1] Christine S T Kansil[2]
Jurusan Hukum, Fakultas Hukum, Univeristas Tarumanagara Jakarta, Kota Jakarta Barat, Provinsi DKI Jakarta, Indonesia[1,2]
Email: vanyaanastasyaa@gmail.com[1] christinek@fh.untar.ac.id[2]

Abstrak

Keamanan siber di Indonesia masih dalam tahap perkembangan dan dihadapkan pada berbagai tantangan yang kompleks. Salah satu tantangan utama adalah ketidakmerataan akses terhadap teknologi dan internet, yang berkontribusi pada kesenjangan digital di masyarakat. Selain itu, pembatasan konten sering kali membatasi kebebasan berekspresi, sedangkan isu privasi dan keamanan data semakin mendesak seiring meningkatnya penggunaan platform digital. Meski pemerintah telah mengambil langkah-langkah positif, seperti penerapan Undang-Undang Perlindungan Data Pribadi, efektivitas regulasi ini masih diragukan karena kurangnya integrasi dalam implementasi. Peningkatan insiden siber, termasuk serangan ransomware yang menargetkan infrastruktur kritis, menyoroti perlunya pendekatan yang lebih holistik dan proaktif. Penelitian ini menekankan pentingnya memperkuat kerangka hukum dan meningkatkan literasi keamanan siber di kalangan masyarakat. Dalam era digital yang terus berubah, mencapai keseimbangan antara liberalisasi dan perlindungan kepentingan nasional sangat penting agar Indonesia dapat memanfaatkan potensi digitalnya secara optimal tanpa mengabaikan aspek keamanan yang krusial.
Kata Kunci: Ancaman siber, Keamanan Siber, Regulasi Kebijakan

Abstract

Cybersecurity in Indonesia is still in its developmental stage and is faced with various complex challenges. One of the main challenges is unequal access to technology and the internet, which contributes to the digital divide in society. In addition, content restrictions often limit freedom of expression, while privacy and data security issues are increasingly pressing as the use of digital platforms increases. While the government has taken positive steps, such as the implementation of the Personal Data Protection Law, the effectiveness of this regulation is still in doubt due to a lack of integration in implementation. The rise in cyber incidents, including ransomware attacks targeting critical infrastructure, highlights the need for a more holistic and proactive approach. This research emphasizes the importance of strengthening the legal framework and improving cybersecurity literacy among the public. In the ever-changing digital era, striking a balance between liberalization and protection of national interests is crucial for Indonesia to optimally harness its digital potential without neglecting crucial security aspects.
Keywords: *Cyber threats, Cybersecurity, Policy regulation.*

PENDAHULUAN

Kerangka hukum keamanan siber di Indonesia masih terus berkembang dan menghadapi berbagai tantangan yang kompleks. Salah satu tantangan utama adalah akses yang tidak merata terhadap teknologi dan internet, yang mengakibatkan kesenjangan digital di antara berbagai lapisan masyarakat. Selain itu, pembatasan konten sering kali menghambat kebebasan berekspresi, sementara isu privasi dan keamanan data semakin mendesak seiring meningkatnya penggunaan platform digital. Literasi digital juga menjadi perhatian, karena banyak individu dan kelompok yang masih kurang memahami cara melindungi diri mereka di dunia maya. Dalam konteks ini, pemahaman dan kesadaran mengenai pentingnya keamanan

siber menjadi kunci untuk membangun masyarakat yang lebih tangguh terhadap ancaman siber.[1] Pemerintah Indonesia telah melakukan sejumlah langkah positif dalam mengembangkan kerangka hukum sibernya, termasuk pemberlakuan Undang-Undang Perlindungan Data Pribadi yang bertujuan untuk melindungi data pribadi warga negara. Namun, efektivitas undang-undang ini masih terbatas, terutama karena adanya fragmentasi dalam implementasi dan pengawasan. Kebijakan yang sering kali diambil sebagai respons terhadap insiden siber juga menunjukkan kurangnya perencanaan yang proaktif. Berbagai insiden siber yang terjadi dalam beberapa tahun terakhir, seperti kebocoran data besar-besaran, semakin menyoroti perlunya pendekatan yang lebih komprehensif dan berkelanjutan dalam menangani isu-isu keamanan siber. Oleh karena itu, upaya untuk memperkuat kerangka hukum dan meningkatkan kesadaran masyarakat menjadi sangat penting untuk menciptakan lingkungan digital yang lebih aman dan terlindungi.[2]

Posisi Indonesia dalam mengatur dunia maya mencerminkan dilema yang kompleks antara liberalisasi dan perlindungan untuk kepentingan nasional. Di satu sisi, upaya untuk meliberalisasi akses dan penggunaan internet sangat penting dalam mendorong inovasi serta pertumbuhan ekonomi digital. Dengan memberikan ruang bagi kreativitas dan pemanfaatan teknologi, Indonesia berpotensi menjadi pusat teknologi dan informasi di kawasan Asia Tenggara. Namun, di sisi lain, tantangan yang muncul dari kebebasan yang terlalu luas dalam dunia maya, seperti penyebaran informasi yang salah, kejahatan siber, dan ancaman terhadap keamanan nasional, mengharuskan pemerintah untuk mengambil langkah-langkah yang lebih tegas dalam mengatur ruang digital.[3] Keseimbangan antara kedua pendekatan ini sangat krusial untuk memastikan bahwa negara ini dapat mempertahankan kedaulatan dan integritasnya. Dalam konteks global yang semakin kompleks, Indonesia perlu mengembangkan kebijakan yang tidak hanya melindungi kepentingan nasional, tetapi juga memberikan kesempatan bagi masyarakat untuk berpartisipasi secara aktif dalam ekonomi digital. Melalui regulasi yang bijaksana, pemerintah dapat menciptakan lingkungan yang mendukung pertumbuhan industri teknologi sambil memastikan keamanan dan perlindungan data bagi warganya. Dengan demikian, Indonesia dapat meraih manfaat maksimal dari potensi digitalnya tanpa mengorbankan aspek-aspek vital yang menyangkut keamanan dan kedaulatan negara.[4] Oleh karena itu, perlindungan hukum terhadap serangan siber merupakan kebutuhan yang mendesak bagi Indonesia. Dalam merinci tantangan yang dihadapi, penting untuk memahami kompleksitas lingkungan digital saat ini, yang terus berkembang dengan cepat seiring dengan kemajuan teknologi. Penggunaan internet yang luas dan meningkatnya transaksi digital telah membawa serta berbagai risiko, termasuk serangan siber yang dapat mengancam privasi individu dan keamanan nasional. Tanpa kerangka hukum yang kuat, individu dan organisasi akan rentan terhadap berbagai ancaman, seperti malware, phishing, dan serangan DDoS, yang tidak hanya merugikan secara finansial tetapi juga dapat merusak reputasi dan kepercayaan publik.[5]

Pengelolaan data dan informasi pribadi di Indonesia dinilai sangat penting untuk diawasi dan dikelola dengan sistem keamanan yang baik dan terjamin. Dalam konteks ini, langkah-langkah proaktif perlu diambil untuk meminimalisir kejahatan seperti pencurian atau pembobolan data, serta praktik ilegal jual beli data dan informasi secara online. Dampak dari kejahatan ini sangat merugikan, karena dapat mengakibatkan penyalahgunaan data dan

[1] Herni Ramayanti , Arief Fahmi Lubis, Peran Hukum dalam Mengatasi Serangan Cyber yang Mengancam Keamanan Nasional, Jurnal Hukum dan HAM Wara Sains Vol. 02, No. 09, 2023, hlm. 905.
[2] *Ibid.* hlm. 905.
[3] *Ibid.* hlm. 905.
[4] *Ibid.* hlm. 905.
[5] Dinda Aprilita Herera , Muhamad Hasan Sebyar, Perlindungan Hukum Terhadap Serangan Siber: Tinjauan Atas Kebijakan Dan Regulasi Terbaru, Jurnal Hukum dan Kewarganegaraan Vol 1 No 5, 2023, hlm. 2.

informasi pribadi oleh pihak yang tidak bertanggung jawab. Oleh karena itu, pengembangan regulasi yang ketat, bersama dengan program edukasi mengenai keamanan siber untuk masyarakat, menjadi krusial dalam menciptakan lingkungan digital yang aman dan melindungi hak-hak individu. Dengan pendekatan yang holistik dan terintegrasi, Indonesia dapat mengatasi tantangan ini dan memperkuat posisi sebagai negara yang aman di dunia maya.[6] Contoh kasus seperti itu terjadi di Pusat Data Nasional (PDN) Kementerian Komunikasi dan Informatika (Kemenkominfo) pada Kamis, 20 Juni 2024, ketika mengalami serangan siber. Serangan ini menyebabkan gangguan pada fasilitas yang mengelola data dari beberapa lembaga pemerintah, termasuk layanan publik seperti layanan imigrasi.[7] Kepala Badan Siber dan Sandi Negara (BSSN), mengkonfirmasi bahwa gangguan pada server PDN disebabkan oleh ransomware. Brain ransomware mengenkripsi data PDN dan menuntut tebusan sebesar 8 juta dolar AS (sekitar Rp131 Miliar). Informasi ini diungkapkan dalam konferensi pers di Gedung Kementerian Komunikasi dan Informatika pada Senin, 24 Juni 2024. Oleh karena itu, pentingnya melindungi infrastruktur penting harus menjadi fokus utama dalam strategi keamanan siber.[8]

Rumusan Masalah

1. Bagaimana efektivitas hukum saat ini dalam menanggapi dan menangani ancaman siber terhadap keamanan negara di Indonesia?
2. Bagaimana kerangka kerja hukum dan kebijakan publik dapat ditingkatkan untuk lebih efektif dalam menghadapi ancaman siber di masa depan?

METODE PENELITIAN

Penelitian ini termasuk dalam kategori penelitian pustaka (library research), yang merupakan jenis penelitian yang fokus pada penggunaan data pustaka sebagai sumber utama informasi. Dalam pendekatan ini, objek kajian terdiri dari berbagai literatur, terutama buku-buku, artikel, dan dokumen tertulis lainnya yang relevan dengan topik yang sedang diteliti. Peneliti memanfaatkan karya-karya ini untuk mengumpulkan data, menganalisis argumen, dan memahami teori-teori yang telah dikembangkan oleh para ahli sebelumnya.[9] Dengan mengandalkan sumber-sumber tertulis, penelitian pustaka memberikan kesempatan bagi peneliti untuk mengeksplorasi berbagai perspektif yang telah ada dalam disiplin ilmu tertentu. Metode ini sangat bermanfaat untuk membangun landasan teoritis yang kuat, karena memungkinkan peneliti untuk menelaah dan mengkritisi temuan-temuan sebelumnya, serta untuk mengidentifikasi celah-celah penelitian yang mungkin belum ditangani. Selama proses penelitian, peneliti tidak hanya mengumpulkan informasi, tetapi juga melakukan analisis kritis terhadap isi dan konteks dari sumber-sumber yang ada. Hal ini penting untuk memastikan bahwa kesimpulan yang diambil adalah valid dan dapat dipertanggungjawabkan. Selain itu, penelitian pustaka juga memungkinkan peneliti untuk membangun argumen yang solid, memperkaya pemahaman terhadap topik yang diteliti, serta menghubungkan ide-ide baru dengan literatur yang sudah ada. Dengan demikian, penelitian pustaka bukan hanya sekadar pengumpulan data, tetapi juga merupakan proses yang melibatkan sintesis informasi dari berbagai sumber, yang akhirnya bertujuan untuk memberikan kontribusi yang berarti dalam pengembangan ilmu pengetahuan dan pemahaman yang lebih mendalam mengenai topik yang dibahas.

---

[6] *Ibid.* hlm. 2.
[7] Kemhan.go.id, https://www.kemhan.go.id/pothan/2024/07/15/keamanan-siber-dan-kebutuhan-sistem-digital-di-dunia-maya.html. Diakses pada Oktober 2024.
[8] *Ibid.*
[9] Sutrisno Hadi, Metodelogi Research, Andi Offset, Yogyakarta, 2002, hlm. 9.

HASIL PENELITIAN DAN PEMBAHASAN

Efektivitas Hukum Saat Ini dalam Menanggapi dan Menangani Ancaman Siber terhadap Keamanan Negara di Indonesia

Hubungan yang rumit antara keamanan siber dan keamanan nasional menggarisbawahi urgensi langkah-langkah hukum yang efektif. Serangan siber dapat membahayakan infrastruktur penting, mengganggu operasi pemerintah, dan membahayakan data sensitif, sehingga menimbulkan ancaman langsung terhadap kedaulatan suatu negara. Ketika negara-negara bergulat dengan integrasi teknologi digital ke dalam layanan-layanan penting, kebutuhan akan kerangka kerja hukum yang kuat menjadi sangat penting.[10] Efektivitas hukum saat ini dalam menangani ancaman siber sangat krusial. Hukum yang ada harus mampu mengakomodasi perkembangan teknologi dan menghadirkan mekanisme yang responsif terhadap serangan siber. Selain itu, penegakan hukum yang konsisten dan kolaborasi antarinstansi menjadi kunci untuk melindungi infrastruktur dan data sensitif dari ancaman yang semakin kompleks. Dengan langkah-langkah hukum yang tepat, Indonesia dapat memperkuat keamanan nasional dan menjaga kedaulatan di era digital ini. Dengan digitalisasi yang semakin pesat dan konektivitas yang semakin meluas, Indonesia kini menghadapi tantangan unik di bidang keamanan siber. Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), yang disahkan pada tahun 2008, berfungsi sebagai instrumen hukum yang mendasar untuk mengatur dan melindungi transaksi digital. Namun, seiring dengan berkembangnya teknologi dan munculnya berbagai bentuk ancaman baru, kritik telah muncul mengenai kecukupan UU ITE dan kemampuannya untuk beradaptasi dengan dinamika ancaman kontemporer yang terus berubah. Oleh karena itu, memahami tantangan dan kekuatan spesifik dari kerangka hukum Indonesia sangat penting agar kita dapat mengajukan rekomendasi yang relevan secara kontekstual. Rekomendasi tersebut harus mampu menjawab kebutuhan masyarakat dan industri, serta memastikan bahwa kebijakan keamanan siber dapat melindungi pengguna tanpa mengorbankan kebebasan berekspresi dan inovasi digital.[11] Dalam konteks efektivitas hukum saat ini dalam menanggapi dan menangani ancaman siber terhadap keamanan negara di Indonesia, UU ITE dapat dianggap sebagai fondasi penting. Namun, efektivitasnya masih dipertanyakan, mengingat tantangan yang terus berkembang seiring dengan pesatnya digitalisasi dan konektivitas. Meskipun UU ITE memberikan kerangka hukum untuk mengatur aktivitas di dunia maya, banyak pihak yang mengkritik bahwa undang-undang ini kurang mampu mengakomodasi berbagai ancaman siber yang semakin kompleks dan beragam, seperti serangan ransomware, pencurian data, dan penyebaran disinformasi.

Peningkatan Kerangka Kerja Hukum dan Kebijakan Publik untuk Lebih Efektif dalam Menghadapi Ancaman Siber di Masa Depan

Kejahatan sibe telah menjadi tantangan serius di era digital ini, yang menuntut adanya peningkatan kerangka kerja hukum dan kebijakan publik agar lebih efektif dalam menghadapi ancaman di masa depan. Permasalahan utama yang muncul dalam konteks ini meliputi beberapa aspek penting.[12] Pertama, kerugian ekonomi akibat kejahatan siber sangat signifikan. Kasus penipuan online, seperti phishing, pencurian identitas, dan penipuan kartu kredit, tidak hanya merugikan individu dan perusahaan secara finansial, tetapi juga menciptakan dampak jangka panjang terhadap kepercayaan konsumen. Serangan siber yang menggunakan malware atau teknik peretasan dapat menyebabkan kerugian besar bagi perusahaan, termasuk pencurian data, perusakan sistem, dan gangguan operasional yang memerlukan biaya besar

[10] Herni Ramayanti , Arief Fahmi Lubis, *Op.Cit,* hlm. 906-907.
[11] *Ibid.* hlm. 907.
[12] Afifah Rizqy Widianingrum, Analisis Implementasi Kebijakan Hukum Terhadap Penanganan Kejahatan Siber Di Era Digital, Journal Iuris Scientia, Vol. 2 No. 2, 2024, hlm. 93.

untuk pemulihan. Oleh karena itu, perlu adanya regulasi yang lebih ketat dan kerangka hukum yang adaptif untuk melindungi aset ekonomi digital.[13] Kedua, masalah keamanan dan privasi menjadi perhatian utama. Pelanggaran data pribadi dan perusahaan yang semakin sering terjadi menyebabkan informasi sensitif jatuh ke tangan yang salah, yang mengakibatkan risiko terhadap privasi individu dan keamanan perusahaan. Serangan siber terhadap infrastruktur kritikal, seperti sistem perbankan, energi, dan komunikasi, tidak hanya mengancam keamanan nasional tetapi juga stabilitas sosial. Kebijakan publik yang menjamin perlindungan data dan privasi menjadi sangat mendesak, termasuk penerapan sanksi yang tegas bagi pelanggar.[14]

Ketiga, kompleksitas hukum dan regulasi menjadi tantangan tersendiri. Hukum yang ada sering kali tidak dapat mengikuti perkembangan teknologi yang cepat, menyebabkan kesenjangan dalam regulasi dan penegakan hukum terhadap kejahatan siber. Penanganan kejahatan siber memerlukan koordinasi yang efektif antara berbagai lembaga penegak hukum, baik di tingkat nasional maupun internasional. Keterlibatan sektor swasta dalam penyusunan regulasi juga penting agar kebijakan yang diambil dapat relevan dengan perkembangan teknologi terkini.[15] Keempat, kesadaran dan literasi digital di masyarakat masih rendah. Banyak masyarakat yang belum sepenuhnya menyadari risiko kejahatan siber dan cara melindungi diri, sehingga mereka rentan terhadap serangan siber. Program edukasi dan kampanye literasi digital yang komprehensif diperlukan untuk meningkatkan kesadaran masyarakat tentang langkah-langkah pencegahan yang efektif. Selain itu, kolaborasi antara pemerintah, lembaga pendidikan, dan sektor swasta dapat mendorong peningkatan kemampuan masyarakat dalam menghadapi ancaman siber.[16] Kelima, terdapat hambatan teknis dalam penanganan kejahatan siber. Teknologi keamanan siber yang ada sering kali tidak mampu mengimbangi metode serangan siber yang semakin canggih, menciptakan celah yang dapat dieksploitasi oleh pelaku kejahatan. Investasi dalam penelitian dan pengembangan teknologi keamanan siber yang inovatif menjadi krusial. Selain itu, perluasan sumber daya manusia yang terlatih dalam bidang keamanan siber dan teknologi informasi juga sangat diperlukan untuk memperkuat pertahanan terhadap kejahatan siber.[17]

Terakhir, tantangan penegakan hukum terkait kejahatan siber cukup besar. Identifikasi dan penangkapan pelaku kejahatan siber sering kali sulit karena mereka dapat beroperasi dari lokasi yang berbeda-beda dan menggunakan teknik yang menyulitkan pelacakan. Proses hukum yang lambat dan birokrasi yang berbelit-belit juga dapat menghambat penanganan kasus kejahatan siber, mengurangi efektivitas penegakan hukum. Oleh karena itu, reformasi hukum yang mendukung respons cepat terhadap kejahatan siber sangat diperlukan.[18] Permasalahan-permasalahan ini menunjukkan kompleksitas dan urgensi dalam penanganan kejahatan siber, yang memerlukan pendekatan komprehensif dan kolaboratif dari berbagai pihak. Hanya dengan meningkatkan kerangka kerja hukum dan kebijakan publik, serta melibatkan semua elemen masyarakat, kita dapat membangun sistem yang lebih tangguh dalam menghadapi ancaman siber di masa depan.[19] Perubahan sosial yang cepat, seperti urbanisasi dan globalisasi, serta penetrasi internet yang tinggi, menciptakan ekosistem di mana kejahatan siber dapat berkembang.[20] Teknologi yang semakin terhubung juga memperbesar risiko kebocoran data dan serangan siber. Masyarakat yang semakin bergantung pada

[13] *Ibid.* hlm. 93.
[14] *Ibid.* hlm. 93.
[15] *Ibid.* hlm. 93.
[16] *Ibid.* hlm. 93.
[17] *Ibid.* hlm. 93.
[18] *Ibid.* hlm. 93.
[19] *Ibid.* hlm. 93.
[20] N. P. S. Meinarni, "Tinjauan Yuridis Cyber Bullying Dalam Ranah Hukum Indonesia," Jurnal Ilmu Sosial Dan Humaniora, Vol. 2 No. 1, 2019.

teknologi informasi dan komunikasi menghadapi risiko keamanan yang meningkat, terutama karena banyaknya data pribadi yang tersimpan secara digital.[21]

KESIMPULAN

Kesimpulan dari penelitian ini adalah hubungan antara keamanan siber dan keamanan nasional di Indonesia menunjukkan kebutuhan mendesak akan langkah-langkah hukum yang efektif, terutama di tengah pesatnya digitalisasi dan ancaman siber yang semakin kompleks. Meskipun Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) telah berfungsi sebagai fondasi hukum, efektivitasnya dipertanyakan dalam menghadapi tantangan baru seperti ransomware dan disinformasi. Oleh karena itu, penting untuk merevisi dan memperkuat kerangka hukum agar mampu melindungi infrastruktur penting dan data sensitif tanpa mengorbankan kebebasan berekspresi serta inovasi digital, sekaligus menjaga kedaulatan negara di era digital. Kejahatan siber telah menjadi tantangan serius di era digital, memerlukan peningkatan kerangka hukum dan kebijakan publik yang lebih efektif untuk menghadapinya. Kerugian ekonomi yang signifikan, masalah keamanan dan privasi, serta kompleksitas hukum menjadi isu utama yang perlu ditangani. Kesadaran masyarakat yang rendah terhadap risiko siber, hambatan teknis dalam teknologi keamanan, dan tantangan penegakan hukum semakin memperburuk situasi. Oleh karena itu, dibutuhkan pendekatan komprehensif dan kolaboratif dari berbagai pihak, termasuk pemerintah, sektor swasta, dan masyarakat, untuk menciptakan sistem yang lebih kuat dalam menghadapi ancaman siber di masa depan, terutama di tengah perubahan sosial yang cepat dan ketergantungan yang semakin tinggi pada teknologi informasi.

Saran

Untuk mengatasi tantangan kejahatan siber yang semakin kompleks di Indonesia, perlu adanya revisi dan penguatan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) agar lebih efektif melindungi infrastruktur penting dan data sensitif. Selain itu, pendekatan komprehensif yang melibatkan pemerintah, sektor swasta, dan masyarakat sangat penting untuk meningkatkan kesadaran akan risiko siber, memperbaiki penegakan hukum, dan mengatasi masalah teknis dalam keamanan. Dengan langkah-langkah ini, Indonesia dapat menciptakan sistem pertahanan yang lebih kuat dan menjaga kedaulatan negara di era digital yang terus berkembang.

DAFTAR PUSTAKA

Afifah Rizqy Widianingrum. Analisis Implementasi Kebijakan Hukum Terhadap Penanganan Kejahatan Siber Di Era Digital. Journal Iuris Scientia. 2(2).

Dinda Aprilita Herera, Muhamad Hasan Sebyar. Perlindungan Hukum Terhadap Serangan Siber: Tinjauan Atas Kebijakan Dan Regulasi Terbaru. Jurnal Hukum dan Kewarganegaraan. 1(5).

Eko Budi, Dwi Wira, and Ardian Infantono. 2021. "Strategi Penguatan Cyber Security Guna Mewujudkan Keamanan Nasional Di Era Society 5.0". Prosiding Seminar Nasional Sains Teknologi dan Inovasi Indonesia (SENASTINDO). 3.

Herni Ramayanti, Arief Fahmi Lubis. 2023. Peran Hukum dalam Mengatasi Serangan Cyber yang Mengancam Keamanan Nasional, Jurnal Hukum dan HAM Wara Sains. 02(9).

Kemhan.go.id, https://www.kemhan.go.id/pothan/2024/07/15/keamanan-siber-dan-kebutuhan-sistem-digital-di-dunia-maya.html.

[21] Eko Budi, Dwi Wira, and Ardian Infantono, "Strategi Penguatan Cyber Security Guna Mewujudkan Keamanan Nasional Di Era Society 5.0," Prosiding Seminar Nasional Sains Teknologi dan Inovasi Indonesia (SENASTINDO), Vol. 3, 2021.

N. P. S. Meinarni. 2019. "Tinjauan Yuridis Cyber Bullying Dalam Ranah Hukum Indonesia," Jurnal Ilmu Sosial Dan Humaniora. 2(1).
Sutrisno Hadi. 2002. Metodelogi Research. Andi Offset. Yogyakarta.