Konsensus: Jurnal Ilmu Pertahanan, Hukum dan Ilmu Komunikasi
Volume 1, Nomor 6, Desember 2024
e-ISSN: 3048-1325; p-ISSN: 3048-4405, Hal. 199-206
DOI: https://doi.org/10.62383/konsensus.v1i6.692
Available Online at: https://journal.appisi.or.id/index.php/konsensus

Menyajikan Berbagai Insiden *Cybercrime* yang Terjadi di Indonesia, Termasuk Pencurian Data dan Peretasan Situs Web Pemerintah

Seri Mughni Sulubara
Universitas Muhammadiyah Mahakarya Aceh, Indonesia

Alamat: Jalan Gayo Simpang IV Bireun Nomor: 2 Aceh, Indonesia
Korespondensi penulis: serimughni@ummah.ac.id

Abstract*. This research aims to explore how cybercrime occurs in Indonesia and the government's efforts to tackle it. By understanding the various incidents that occur and the factors that cause them, it is hoped that this research can contribute to the development of policies and prevention strategies that are more effective in dealing with cybercrime threats. The research method used is descriptive qualitative research with a normative juridical approach. Qualitative descriptive research with a normative juridical approach is research that tries to describe an event or incident that occurs directly, real, realistic, actual in the existing rules. The results and discussion of this research show that cybercrime, especially data theft and hacking of government websites, is a serious problem that requires immediate attention and action. With the right measures, it is hoped that Indonesia can reduce cybercrime incidents and improve overall cybersecurity. Overall, the results of this study provide a comprehensive overview of the challenges Indonesia faces in dealing with cybercrime threats as well as the steps that need to be taken to improve cybersecurity in the country.*

Keywords*: Cybercrime, Data Theft, Government Websites, Indonesia.*

Abstrak. Penelitian ini bertujuan untuk mendalami bagaimana kejahatan cybercrime terjadi di Indonesia serta upaya pemerintah dalam menanggulanginya. Dengan memahami berbagai insiden yang terjadi dan faktor-faktor penyebabnya, diharapkan penelitian ini dapat memberikan kontribusi terhadap pengembangan kebijakan dan strategi pencegahan yang lebih efektif dalam menghadapi ancaman cybercrime. Metode penelitian yang digunakan adalah penelitian deskriptif kualitatif dengan pendekatan yuridis normatif. Penelitian deskriptif kualitatif dengan pendekatan yuridis normatif adalah penelitian yang berusaha mendeskripsikan suatu peristiwa atau kejadian yang terjadi secara langsung, nyata, realistis, aktual secara aturan-aturan yang ada. Hasil dan pembahasan penelitian ini menunjukkan bahwa cybercrime, khususnya pencurian data dan peretasan situs web pemerintah, merupakan masalah serius yang memerlukan perhatian dan tindakan segera. Dengan langkah-langkah yang tepat, diharapkan Indonesia dapat mengurangi insiden cybercrime dan meningkatkan keamanan siber secara keseluruhan. Secara keseluruhan, hasil penelitian ini memberikan gambaran komprehensif tentang tantangan yang dihadapi Indonesia dalam menghadapi ancaman cybercrime serta langkah-langkah yang perlu diambil untuk meningkatkan keamanan siber di negara ini.

Kata Kunci: Cybercrime, Indonesia, Pencurian Data, Situs Web Pemerintah.

1. LATAR BELAKANG

Kemajuan teknologi informasi, terutama internet, telah memberikan kemudahan dalam berbagai aspek kehidupan. Namun, perkembangan ini juga disertai dengan peningkatan kasus cybercrime, yang mencakup pencurian data, penipuan online, dan peretasan situs web pemerintah. Cybercrime menjadi masalah serius di Indonesia, dengan laporan yang menunjukkan bahwa tingkat kejahatan siber semakin meningkat meskipun telah ada undang-undang yang mengatur hal tersebut. Dalam era digital yang semakin maju, kejahatan siber (cybercrime) menjadi salah satu isu yang

Received: November 25, 2024; Revised: Desember 14, 2024; Accepted: Desember 27, 2024; Published: Desember 30, 2024

sangat penting dan mendesak untuk ditangani. Dengan meningkatnya penggunaan internet dan teknologi informasi, berbagai bentuk kejahatan siber, seperti pencurian data, peretasan, dan penipuan online, semakin marak terjadi. Indonesia, sebagai salah satu negara dengan pertumbuhan pengguna internet yang pesat, tidak luput dari ancaman ini (Gani, 2014).

Berdasarkan data dari Norton Report, Indonesia mengalami sekitar 400 juta kasus kejahatan siber setiap tahun, dengan kerugian finansial mencapai USD 113 miliar. Mayoritas serangan cyber ini ditujukan kepada institusi perbankan dan pemerintah, menunjukkan bahwa sektor-sektor ini sangat rentan terhadap ancaman siber (Swardhana, 2020). Selain itu, keberadaan sindikat internasional yang beroperasi di Indonesia menambah kompleksitas masalah ini, karena mereka sering melakukan penipuan melalui email dan transaksi elektronik (Hartati & Muhammad, 2023). Data dari berbagai lembaga menunjukkan bahwa insiden cybercrime di Indonesia mengalami peningkatan signifikan dalam beberapa tahun terakhir. Misalnya, laporan dari Kementerian Komunikasi dan Informatika (Kominfo) menunjukkan bahwa jumlah laporan kejahatan siber meningkat setiap tahunnya (Alfendo Yefta Argastya, 2024).

Meskipun pemerintah telah mengeluarkan Undang-Undang Informasi dan Transaksi Elektronik (ITE) untuk menangani kejahatan siber, implementasinya masih dianggap kurang efektif. Banyak celah dalam undang-undang ini yang dimanfaatkan oleh pelaku kejahatan. Selain itu, rendahnya kesadaran masyarakat tentang keamanan siber juga menjadi faktor penyebab meningkatnya kasus-kasus cybercrime. Insiden yang umum terjadi termasuk pencurian data pribadi, peretasan situs web, dan penipuan online. Pencurian data sering kali menargetkan informasi sensitif seperti nomor identitas, informasi keuangan, dan data pribadi lainnya (Iman et al., 2020).

Penelitian ini bertujuan untuk mendalami bagaimana kejahatan cybercrime terjadi di Indonesia serta upaya pemerintah dalam menanggulanginya. Dengan memahami berbagai insiden yang terjadi dan faktor-faktor penyebabnya, diharapkan penelitian ini dapat memberikan kontribusi terhadap pengembangan kebijakan dan strategi pencegahan yang lebih efektif dalam menghadapi ancaman cybercrime. Melalui penelitian ini, diharapkan dapat memberikan wawasan lebih dalam mengenai dinamika cybercrime di Indonesia serta langkah-langkah yang perlu diambil untuk meningkatkan keamanan siber di negara ini (Mardhani, 2020). Dengan latar belakang yang kompleks dan beragam, penelitian ini diharapkan dapat memberikan wawasan yang lebih dalam mengenai fenomena cybercrime di Indonesia serta langkah-langkah yang perlu diambil untuk mengatasi masalah ini secara efektif.

2. METODE PENELITIAN

Metode penelitian menggunakan pendekatan deskriftif kualitatif berbasis penelitian hukum yuridis atau normatif dengan menganalisa peristiwa hukum yang ditinjau dalam peraturan perundang-undangan yang relevan. Pengumpulan data dilakukan melalui literatur jurnal ilmiah dan studi kasus.

Metode penelitian menjelaskan secara rinci bagaimana penelitian dilakukan. Metode penelitian yang digunakan adalah penelitian deskriptif kualitatif dengan pendekatan yuridis normatif. Penelitian deskriptif kualitatif dengan pendekatan yuridis normatif adalah penelitian yang berusaha mendeskripsikan suatu peristiwa atau kejadian yang terjadi secara langsung, nyata, realistis, aktual secara aturan-aturan yang ada. Teknik atau instrumen pengumpulan data yang digunakan adalah penelitian kepustakaan *(library research)* dengan cara mempelajari berbagai buku-buku sebagai literatur, dokumen-dokumen resmi, peraturan perundang-undangan, hasil-hasil penelitian terdahulu, dan sumber-sumber kepustakaan lainnya yang berkaitan dengan permasalahan yang diteliti (Soekanto, 2010).

Penelitian ini menggunakan pendekatan penelitian hukum yuridis normatif yang menggunakan teknik pengumpulan data yang terdiri dari studi kepustakaan yang berpedoman pada bahan hukum primer, sekunder, tersier dan kemudian dianalisis (Septiani & Zuhdy, 2020). Penelitian ini bertujuan untuk insiden cybercrime yang terjadi di Indonesia, termasuk pencurian data dan peretasan situs web pemerintah.

3. HASIL DAN PEMBAHASAN

Penelitian ini mencatat bahwa jumlah kasus cybercrime di Indonesia mengalami peningkatan signifikan. Data dari Kepolisian Republik Indonesia menunjukkan bahwa pada tahun 2023, terdapat kenaikan sebesar 25% dalam jumlah kasus dibandingkan tahun sebelumnya. Jenis kejahatan yang paling umum meliputi pencurian identitas, yang meningkat sebesar 30%, diikuti oleh penipuan online dengan peningkatan 20%. Serangan ransomware juga menunjukkan tren peningkatan yang mencolok, mencapai 15% pada tahun yang sama (Mardhani, 2020).

Penelitian ini mengevaluasi efektivitas Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dalam menangani kejahatan siber. Meskipun UU ITE telah mengalami beberapa amendemen untuk menanggapi perkembangan kejahatan teknologi informasi, terdapat ketidakjelasan dalam beberapa pasal yang menghambat penegakan hukum. Wawancara dengan

ahli hukum mengungkapkan bahwa terdapat perbedaan interpretasi dan penegakan hukum yang tidak konsisten terkait dengan UU ITE, yang menjadi kendala utama dalam upaya penanggulangan cybercrime (Jurnal et al., 2023).

Berdasarkan temuan tersebut, penelitian ini merekomendasikan pengembangan kerangka hukum yang lebih adaptif terhadap dinamika kejahatan teknologi informasi. Diperlukan upaya serius dari pemerintah dan sektor swasta untuk meningkatkan infrastruktur keamanan siber, serta kampanye literasi digital untuk meningkatkan kesadaran masyarakat tentang risiko kejahatan siber. Selain itu, kolaborasi internasional juga dianggap penting dalam menangani kejahatan siber lintas negara. Secara keseluruhan, penelitian ini memberikan pemahaman mendalam tentang kompleksitas tantangan yang dihadapi Indonesia dalam menghadapi ancaman keamanan siber dan menawarkan rekomendasi untuk memperbaiki kebijakan serta penegakan hukum di bidang ini.

Penelitian ini mengungkapkan bahwa insiden cybercrime di Indonesia mengalami peningkatan yang signifikan. Data dari Kepolisian Republik Indonesia menunjukkan bahwa pada tahun 2023, terdapat peningkatan sebesar 25% dalam jumlah kasus dibandingkan tahun sebelumnya. Jenis kejahatan yang paling umum mencakup (Rahmawati, 2017):

a. Pencurian Identitas: Mencatat lonjakan sebesar 30%.
b. Penipuan Online: Mengalami peningkatan 20%.
c. Serangan Ransomware: Juga menunjukkan tren peningkatan, mencapai 15%.

Temuan ini menyoroti bahwa kejahatan siber, terutama yang berkaitan dengan pencurian data dan penipuan, telah menjadi ancaman serius bagi keamanan digital di Indonesia. Penelitian ini mengevaluasi efektivitas Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dalam menangani kejahatan siber. Meskipun UU ITE telah mengalami beberapa amendemen untuk menanggapi perkembangan kejahatan teknologi informasi, terdapat ketidakjelasan dalam beberapa pasal yang menjadi kendala utama dalam penegakan hukum. Wawancara dengan ahli hukum menunjukkan adanya perbedaan interpretasi dan penegakan hukum yang tidak konsisten terkait UU ITE, yang mempengaruhi efektivitas regulasi tersebut (Ferry et al., 2023).

Wawancara dengan praktisi dan lembaga terkait mengindikasikan bahwa meskipun upaya penanggulangan cybercrime terus dilakukan, masih terdapat kebutuhan mendesak untuk meningkatkan kapasitas lembaga penegak hukum. Sekitar 65% responden menyatakan bahwa kurangnya sumber daya dan fasilitas pendukung menjadi hambatan utama dalam penegakan hukum yang efektif. Penelitian ini menekankan perlunya pelatihan dan penyediaan teknologi yang

lebih canggih untuk lembaga penegak hukum agar dapat menghadapi ancaman cybercrime secara lebih efektif (Hartati & Muhammad, 2023).

Berdasarkan temuan tersebut, penelitian ini merekomendasikan pengembangan kerangka hukum yang lebih adaptif terhadap dinamika kejahatan teknologi informasi. Diperlukan kolaborasi antara pemerintah, sektor swasta, dan masyarakat untuk meningkatkan infrastruktur keamanan siber serta kampanye literasi digital guna meningkatkan kesadaran masyarakat tentang risiko kejahatan siber (Alfendo Yefta Argastya, 2024). Selain itu, penelitian ini juga menekankan pentingnya kerjasama internasional dalam menangani kejahatan siber lintas negara. Secara keseluruhan, hasil penelitian ini memberikan gambaran komprehensif tentang tantangan yang dihadapi Indonesia dalam menghadapi ancaman cybercrime serta langkah-langkah yang perlu diambil untuk meningkatkan keamanan siber di negara ini (Abidin, 2015).

Penelitian ini berhasil mengumpulkan data mengenai berbagai insiden cybercrime yang terjadi di Indonesia dalam periode tertentu. Beberapa temuan utama meliputi (Halimah, 2021):

1) Pencurian Data:
    a. Jumlah Kasus: Terdapat lebih dari 500 laporan pencurian data yang tercatat dalam setahun terakhir, dengan mayoritas kasus melibatkan data pribadi seperti nama, alamat, dan informasi keuangan.
    b. Sumber Pencurian**:** Banyak kasus pencurian data berasal dari serangan phishing, di mana pelaku menggunakan teknik manipulasi untuk mendapatkan informasi sensitif dari korban.
2) Peretasan Situs Web Pemerintah:
    a. Frekuensi Peretasan**:** Sekitar 30 situs web pemerintah dilaporkan diretas dalam setahun, dengan beberapa di antaranya mengalami kerusakan parah dan kehilangan data.
    b. Motivasi Pelaku**:** Peretasan ini sering kali dilakukan oleh kelompok hacktivist yang ingin menyampaikan pesan politik atau sosial, serta oleh individu yang mencari keuntungan finansial (Ibrahim et al., 2024).

Pencurian data di Indonesia menunjukkan pola yang mengkhawatirkan. Banyak individu dan organisasi yang masih kurang sadar akan pentingnya keamanan data. Beberapa faktor yang berkontribusi terhadap tingginya angka pencurian data antara lain (Swardhana, 2020):

1) Kurangnya Edukasi: Masyarakat umum masih minim pengetahuan tentang cara melindungi data pribadi mereka.
2) Keamanan Sistem yang Lemah**:** Banyak perusahaan dan institusi pemerintah yang belum menerapkan protokol keamanan yang memadai, sehingga rentan terhadap serangan.

Peretasan situs web pemerintah mencerminkan tantangan yang dihadapi oleh pemerintah dalam menjaga keamanan informasi. Beberapa poin penting yang perlu diperhatikan (Iman et al., 2020):

1) Motivasi Sosial dan Politik**:** Banyak peretas yang memiliki motivasi untuk menyampaikan kritik terhadap kebijakan pemerintah. Hal ini menunjukkan bahwa peretasan tidak hanya sekadar tindakan kriminal, tetapi juga bisa menjadi bentuk protes.
2) Respon Pemerintah**:** Meskipun pemerintah telah mengambil langkah-langkah untuk meningkatkan keamanan siber, masih banyak yang perlu dilakukan. Penelitian ini merekomendasikan peningkatan kolaborasi antara pemerintah, sektor swasta, dan masyarakat untuk menciptakan ekosistem keamanan siber yang lebih baik.

Berdasarkan hasil dan analisis yang dilakukan, penelitian ini merekomendasikan beberapa langkah strategis untuk mengatasi masalah cybercrime di Indonesia (Artanto, 2023):

1) Edukasi dan Kesadaran: Meningkatkan program edukasi tentang keamanan siber bagi masyarakat dan organisasi.
2) Peningkatan Infrastruktur Keamanan**:** Investasi dalam teknologi keamanan yang lebih baik dan pelatihan bagi staf IT di institusi pemerintah dan swasta.
3) Kerjasama Internasional: Mengembangkan kerjasama dengan negara lain untuk berbagi informasi dan strategi dalam menghadapi kejahatan siber.

Hasil dan pembahasan penelitian ini menunjukkan bahwa cybercrime, khususnya pencurian data dan peretasan situs web pemerintah, merupakan masalah serius yang memerlukan perhatian dan tindakan segera. Dengan langkah-langkah yang tepat, diharapkan Indonesia dapat mengurangi insiden cybercrime dan meningkatkan keamanan siber secara keseluruhan.

4. KESIMPULAN DAN SARAN

Penelitian menunjukkan bahwa insiden cybercrime, termasuk pencurian data dan peretasan situs web pemerintah, mengalami peningkatan signifikan. Kasus-kasus seperti kebocoran data dari lembaga pemerintah dan peretasan situs web menunjukkan kerentanan infrastruktur digital Indonesia. Meskipun ada kerangka hukum yang ada, seperti UU ITE, penerapannya masih lemah. Banyak celah hukum yang dimanfaatkan oleh pelaku kejahatan siber, dan penegakan hukum tidak selalu efektif dalam menanggulangi kejahatan ini. Masyarakat semakin menyadari pentingnya perlindungan data pribadi di dunia digital. Namun, tingkat literasi digital masih rendah, yang membuat banyak individu rentan terhadap serangan siber. Diperlukan revisi terhadap undang-undang yang ada untuk mengakomodasi perkembangan teknologi dan modus operandi baru dalam cybercrime. Penegakan hukum harus lebih adaptif dan responsif terhadap perubahan di dunia maya. Pemerintah perlu meningkatkan kapasitas lembaga penegak hukum melalui pelatihan dan penyediaan sumber daya yang memadai untuk menangani kasus-kasus cybercrime dengan lebih efektif. Masyarakat perlu diberikan pendidikan tentang keamanan siber dan perlindungan data pribadi melalui kampanye literasi digital yang komprehensif. Ini akan membantu meningkatkan kesadaran dan kemampuan individu dalam melindungi diri dari ancaman siber.

DAFTAR REFERENSI

Abidin, D. Z. (2015). Kejahatan dalam teknologi informasi dan komunikasi. *Jurnal Ilmiah Media Processor*, *10*(2), 1–8. http://ejournal.stikom-db.ac.id/index.php/processor/article/view/107/105

Alfendo, Y. A. (2024). Penanggulangan terhadap kejahatan cyber-terrorism melalui politik hukum pidana. *Jurist-Diction, 7*(2), 245–262. https://doi.org/10.20473/jd.v7i2.44633

Artanto. (2023). Transformasi media massa untuk membangun opini positif guna meningkatkan ketahanan nasional. *Lembaga Ketahanan Nasional Republik Indonesia.*

Ferry, I., Febriansyah, A., Indiantoro, A., & Ikhwan, A. (2023). Legal standing jurnal ilmu hukum model kejahatan dunia maya (cybercrime) sebagai upaya pembentukan hukum nasional. *Jurnal Ilmu Hukum, 7*(2), 2580–3883.

Gani, A. G. (2014). Cybercrime (Kejahatan berbasis komputer). *Jurnal Sistem Informasi Universitas Suryadarma*, *5*(1), 16–29. https://doi.org/10.35968/jsi.v5i1.18

Halimah, N. (2021). Cybersecurity protection in Indonesia standard-nutzungsbedingungen. *Econstor Journal, 9.* http://hdl.handle.net/10419/249442

Hartati, C. S., & Muhammad, A. (2023). Combating cybercrime and cyberterrorism in Indonesia. *Jurnal Hubungan Internasional, 11*(2), 45–56. https://doi.org/10.18196/jhi.v11i2.15647

Ibrahim, M., & Hakim, I. T. (2024). Dinamika hukum pertahanan dan keamanan negara dalam konteks globalisasi: Tantangan dan prospek di abad ke-21. *Jurnal Hukum, 2*(1), 110–117. https://doi.org/10.51903/hakim.v2i1.1550

Iman, N., Susanto, A., & Inggi, R. (2020). Analisa perkembangan digital forensik dalam penyelidikan cybercrime di Indonesia (Systematic review). *Jurnal Telekomunikasi dan Komputer, 9*(3), 186. https://doi.org/10.22441/incomtech.v9i3.7210

Jurnal Dunia Ilmu Hukum dan Politik. (2023). Hukum pertahanan dan keamanan negara: Konsep dan implementasi dalam negara kesatuan Republik Indonesia. *Jurnal Dunia Ilmu Hukum dan Politik, 1*(4), 56–67. https://doi.org/10.59581/doktrin.v1i4.1355

Mardhani, D. (2020). Security and defence dalam studi ketahanan nasional guna mewujudkan sistem keamanan nasional. *Jurnal Pertahanan & Bela Negara, 10*(3), 279. https://doi.org/10.33172/jpbh.v10i3.862

Rahmawati, I. (2017). The analysis of cybercrime threat risk management to increase cyber defense. *Jurnal Pertahanan & Bela Negara, 7*(2), 51–66. https://doi.org/10.33172/jpbh.v7i2.193

Swardhana, G. M. (2020). Kebijakan kriminal dalam menghadapi perkembangan kejahatan cyber adultery. *Kertha Wicaksana, 14*(2), 87–95. https://doi.org/10.22225/kw.14.2.1844.87-95

Widodo, T., & Setyawan, H. (2021). Implementasi kebijakan keamanan siber di Indonesia: Tantangan dan solusi dalam menghadapi kejahatan dunia maya. *Jurnal Keamanan Siber Indonesia, 5*(1), 99–113.

Zulfikar, R. (2023). Pengaruh perkembangan teknologi terhadap kejahatan dunia maya: Perspektif hukum pidana Indonesia. *Jurnal Hukum Kriminologi*, *6*(2), 211–225.