KIRANA : Social Science Journal
Volume 2, Number 1, 2025 pp. 1-5
E-ISSN : 3062-780X
DOI https://doi.org/10.61579/kirana.v2i1.227
Open Access: https://ejournal.sagita.or.id/index.php/kirana

Analisis Hukum Pidana Atas Keamanan Data Dan Serangan Siber Terhadap Pertahanan Nasional

Sri Hasrina[1*], Inda Sari[2] , Thiara Tri Funny Manguma[3] , Emil Fatra[4]
[1,2] Department of Law, Almarisah Madani University, Makassar, Indonesia
[3]Department of Informatic, Almarisah Madani University, Makassar, Indonesia
[4]Department of Communication, Almarisah Madani University, Makassar, Indonesia
Corresponding Email : srihasrina9@gmail.com

ARTICLEINFO
Article history:
30 October 2024
Received in revised form
13 November 2024
Accepted 29 December 2024
Available online 06 January 2025

Kata Kunci:
Keamanan Data, Serangan Siber, Pertahanan Nasional, Hukum Pidana

Keywords:
Data Security, Cyber Attacks, National Defense,Criminal Law

ABSTRAK

Seiring perkembangan teknologi digital, ancaman siber menjadi semakin kompleks dan memiliki dampak signifikan terhadap keamanan negara. Serangan siber, yang mencakup pencurian data, perusakan sistem, hingga pengambilalihan infrastruktur penting, menimbulkan tantangan baru dalam menjaga stabilitas nasional. Dalam konteks hukum pidana, penanganan serangan siber membutuhkan regulasi yang mampu menjawab tantangan ancaman teknologi tinggi ini, baik dari segi pencegahan maupun penindakan. Penelitian ini bertujuan untuk mengidentifikasi aspek-aspek hukum pidana yang relevan dalam melindungi keamanan data dan menganalisis kerangka hukum yang ada, termasuk efektivitas, kelemahan, serta potensi pengembangan hukum dalam merespons ancaman siber. Melalui pendekatan normatif, penelitian ini juga mengevaluasi upaya perlindungan terhadap data dan infrastruktur kritis, dengan melihat perbandingan dari beberapa negara lain. Hasil penelitian ini diharapkan dapat memberikan kontribusi dalam perumusan kebijakan hukum pidana yang lebih komprehensif untuk melindungi kepentingan nasional dari ancaman siber.

ABSTRACT

As digital technology advances, cyber threats are becoming increasingly complex and have a significant impact on national security. Cyber attacks, including data theft, system destruction, and takeover of critical infrastructure, pose new challenges in maintaining national stability. In the context of criminal law, handling cyber attacks requires regulations that are able to answer the challenges of this high-tech threat, both in terms of prevention and enforcement. This study aims to identify aspects of criminal law that are relevant in protecting data security and analyze the existing legal framework, including the effectiveness, weaknesses, and potential for legal development in responding to cyber threats. Through a normative approach, this study also evaluates efforts to protect critical data and infrastructure, by looking at comparisons from several other countries. The results of this study are expected to contribute to the formulation of more comprehensive criminal law policies to protect national interests from cyber threats.

1. INTRODUCTION

Beberapa negara telah memiliki satuan pasukan siber khusus dalam pertahanan dan keamanan negaranya. Badan atau organisasi tersebut bertugas untuk menghimpun segala upaya pertahanan dan serangan balik terhadap keamanan siber dan sistem jaringannya (Sa'diyah & Vinata, 2016). Melihat kekuatan dan ancaman yang dapat terjadi akibat kemajuan teknologi informasi, banyak negara mulai membangun pasukan perang siber (Umra, 2019),

* *Corresponding Author: Sri Hasrina: srihasrina9@gmail.com*

karena perang ini bukan lagi sekadar permainan virtual dan cerita fiksi, tetapi telah menjadi bagian dari papan catur dunia yang menyebutnya sebagai 'dimensi kelima peperangan', negara juga diharapkan mampu menginisiasi suatu regulasi di bidang siber (cyber law) yang lebih kuat dan berdampak global (Soewardi, 2013). Dengan adanya hukum siber yang tegas di dunia internasional, diharapkan mampu meredam maraknya kejahatan di dunia siber. Sebelum hal tersebut terlaksana, alangkah lebih bijaknya jika Indonesia menata kembali penguasaan teknologi dan membuat undang-undang khusus terkait ancaman siber selain di darat, laut, udara, dan ruang angkasa (Manurung, 2024). Pasalnya, inovasi teknologi tengah mengubah taktik peperangan modern, menjadikan dunia maya sebagai garis depan pertempuran. Menjadikan dunia maya sebagai dimensi kelima perang cukup beralasan (A, 2019), karena semua negara pasti ingin meningkatkan kemampuannya dalam melindungi diri dari serangan musuh. Pesatnya kemajuan teknologi informasi dan komunikasi saat ini akan menjadi landasan penting bagi pengembangan doktrin militer di masa mendatang. Dengan demikian, teknologi informasi dan komunikasi akan sangat memengaruhi perubahan strategi militer.

Tantangan keamanan tersebut sangat serius dan dapat memengaruhi pertahanan Negara (Bakrie et al., 2022), sehingga Direktorat Pertahanan Sinyal Departemen Pertahanan Australia telah membentuk sebuah badan yang disebut Pusat Operasi Keamanan Siber (CSOC) yang bertanggung jawab untuk mendeteksi dan menanggulangi ancaman kejahatan siber terhadap kepentingan dan pemerintahan Australia. Yang terbaru adalah Tiongkok yang juga telah membentuk pasukan siber. Pasukan tersebut diberi nama "Tentara Biru", pasukan ini bertugas untuk melindungi negara dari serangan siber. Pasukan digital ini akan ditempatkan di kawasan militer Guangzhou, sebelah selatan Tiongkok. Inggris juga tengah membangun pertahanan siber. Sistem yang disebut Pusat Operasi Keamanan Siber (CSOC) (Admi & Maulana, 2020) tersebut berlokasi di Markas Besar Komunikasi Pemerintah Inggris (GCHQ), di Cheltenham, sekitar 160 kilometer di sebelah barat laut London. Dengan berbagai kasus kejahatan siber di Indonesia, stabilitas keamanan dan ketertiban nasional menghadapi ancaman yang signifikan. Eskalasi kejahatan siber telah mencapai level yang cukup tinggi(Karisma, 2023). Penanganan tindakan melawan hukum di dunia maya tidak mudah hanya dengan hukum positif konvensional. Hal ini disebabkan oleh hubungan yang kompleks antara lima faktor yang saling terkait, yaitu pelaku, korban kejahatan, reaksi sosial terhadap kejahatan, dan hokum (Mamluchah & Mubarok, 2020). Meskipun hukum memiliki peran penting dalam pencegahan dan penanggulangan kejahatan, namun menciptakan regulasi hukum yang responsif terhadap berbagai bidang hukum yang berubah dengan cepat seperti teknologi informasi bukanlah tugas yang mudah. Dalam menghadapi tantangan kejahatan dunia maya, diperlukan kerja sama lintas sektor, meliputi pemerintah, lembaga penegak hukum, sektor swasta, dan masyarakat secara keseluruhan. Selain itu, pengembangan kerangka hukum yang adaptif dan penggunaan teknologi keamanan siber yang canggih menjadi penting dalam memerangi kejahatan dunia maya yang terus berkembang.

2. METHOD

Penelitian ini merupakan penelitian normatif yang bersifat deskriptif analisis yaitu penelitian yang bermaksud memberikan gambaran tentang suatu fenomena sosial yang bertujuan memberikan gambaran secara sistematis, faktual, dan akurat (Husain et al., 2020), dilakukan dengan pendekatan hukum yaitu menganalisis norma hukum yang ada secara sah

dengan menggunakan peraturan perundang-undangan yang berlaku dan teori hukum yang didukung oleh studi data kepustakaan. Penelitian normatif dilakukan dengan cara mengumpulkan dan menganalisis bahan hukum primer (Benuf et al., 2019) yaitu Undang-Undang Nomor 19 Tahun 2016 Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik yang Aman, Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Keamanan Informasi Elektronik yang Bersifat Rahasia, Peraturan Menteri Pertahanan Nomor 54 Tahun 2020 tentang Keamanan Sistem Informasi Pertahanan dan bahan hukum sekunder yaitu bahan hukum yang membantu menganalisis, memahami, dan menjelaskan bahan hukum primer seperti buku, jurnal ilmiah, artikel, tesis, makalah, dan penelusuran di internet (Disemadi, 2022). Hasil yang diperoleh melalui studi kepustakaan disusun secara sistematis dengan analisis deskriptif kualitatif dengan cara menguraikan secara keseluruhan hasil yang diperoleh dari bahan hukum dikaitkan dengan rumusan peraturan perundang-undangan yang ada dan dapat ditarik simpulan atau jawaban untuk menjawab permasalahan yang diteliti oleh penulis.

3. RESULT AND DISCUSSION

Analisis hukum pidana terhadap keamanan data dan serangan siber terhadap pertahanan negara menunjukkan bahwa perlindungan data pribadi dan infrastruktur nasional menjadi prioritas utama dalam menghadapi tantangan digital modern. Perlindungan hukum yang efektif dan penegakan hukum yang kuat menjadi kunci dalam menanggapi ancaman serius terhadap keamanan nasional ini. Penangkalan terhadap pelaku dengan sanksi pidana yang berat dan tegas terhadap pelaku serangan siber dapat menjadi penangkalan yang efektif untuk mencegah serangan serupa di masa mendatang. Ancaman hukuman yang berat dapat membuat pelaku berpikir dua kali sebelum melakukan serangan yang dapat membahayakan keamanan data dan pertahanan negara. Penegakan hukum yang efektif dalam memberikan perlindungan terhadap data dari serangan siber memerlukan penegakan hukum yang efektif terhadap pelaku kejahatan siber. Sanksi pidana yang jelas dan tegas bagi pelaku serangan siber dapat memperkuat penegakan hukum dalam menangani kasus serangan tersebut, sehingga memberikan perlindungan yang lebih baik bagi keamanan data dan pertahanan negara. Pengembangan hukum pidana yang relevan dapat memberikan perlindungan terhadap keamanan data dari serangan siber dalam konteks pertahanan negara memerlukan keberadaan lembaga hukum yang relevan dan berkualitas. Hal ini termasuk perumusan undang-undang yang jelas dan komprehensif tentang kejahatan siber serta penegakan hukum yang konsisten dan efektif untuk melindungi keamanan nasional. Hukuman pidana juga harus memberikan perlindungan khusus bagi infrastruktur penting yang rentan terhadap serangan siber, seperti sistem komunikasi, sistem keuangan, dan sistem transportasi. Ancaman hukuman berat bagi pelaku serangan terhadap infrastruktur penting dapat membantu meminimalkan risiko terhadap keamanan nasional.

Kolaborasi antara pemerintah dan sektor swasta juga diperlukan untuk meningkatkan efektivitas hukuman pidana dalam melindungi keamanan data dari serangan siber. Kolaborasi antara pemerintah dan sektor swasta juga sangat penting. Hal ini mencakup kerja sama dalam pelaporan dan penanganan insiden keamanan data, serta pembentukan kerangka kerja

bersama untuk memerangi ancaman siber secara lebih efektif. Dalam konteks hukum pidana, tindakan yang dapat dianggap sebagai serangan siber terhadap pertahanan nasional meliputi:

a. Cyber Spying: Pengumpulan atau infiltrasi untuk mencuri informasi sensitif yang dapat membahayakan keamanan nasional.
b. Critical Infrastructure Destruction: Upaya untuk merusak atau menghancurkan infrastruktur penting seperti sistem komunikasi, listrik, atau transportasi.
c. PsyOps: Penyebaran informasi atau propaganda palsu untuk memengaruhi stabilitas dalam negeri atau opini publik.

4. CONCLUSION

Di era digital saat ini, data menjadi salah satu aset penting yang harus dilindungi, terutama bagi sektor pertahanan. Keamanan data yang kuat diperlukan untuk menghindari kebocoran informasi yang dapat mengancam kedaulatan negara. Sistem pertahanan yang rentan terhadap serangan siber dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab untuk melakukan spionase atau sabotase, yang berpotensi melemahkan stabilitas negara.

Penelitian ini menganalisis aspek hukum pidana yang terkait dengan serangan siber dan langkah-langkah hukum yang dapat diambil untuk menangani kasus pelanggaran keamanan data dalam konteks pertahanan nasional. Berdasarkan penelitian, diketahui bahwa regulasi yang ada masih perlu disesuaikan dengan perkembangan teknologi dan kompleksitas serangan siber. Kejahatan siber yang semakin canggih memerlukan hukum pidana yang tangguh dan responsif dalam menjamin keamanan data di sektor pertahanan. Selain itu, ketentuan pidana yang relevan perlu diperkuat dengan penegakan hukum yang efektif agar mampu mencegah dan menindak kejahatan siber secara optimal.

Secara keseluruhan, penelitian ini menekankan pentingnya pembaruan regulasi yang mendukung pengamanan data strategis negara dalam menghadapi ancaman siber. Kolaborasi antara pemerintah, pihak militer, dan badan hukum diperlukan untuk membentuk sistem pertahanan siber yang solid. Dengan peraturan hukum pidana yang komprehensif dan penegakan yang konsisten, Indonesia dapat memperkuat ketahanan nasionalnya dari serangan siber, sehingga kedaulatan dan keamanan nasional tetap terjaga.

5. ACKNOWLEDGE

Terima kasih kepada lembaga dan pimpinan jurnal KIRANA yang telah memberikan kesempatan untuk menjadi bagian dari jurnal tersebut, jurnal ini dibuat secara mandiri sebagai salah satu kewajiban dalam tridarma perguruan tinggi.

6. REFERENCES

A, F. N. A. (2019). *Prosiding Seminar Nasional 2019 " Selamat Datang Era Post Truth : Apa dan Bagaimana ?"*

Admi, A., & Maulana, A. H. N. (2020). Penerapan Elastic Stack sebagai Tools Alternatif Pemantauan Traffic Jaringan dan Host pada Instansi Pemerintah untuk Memperkuat Keamanan dan Ketahanan Siber Indonesia. *JUSTINDO (Jurnal Sistem Dan Teknologi Informasi Indonesia)*, *5*(2), 69–77. https://doi.org/10.32528/justindo.v5i2.3527

Bakrie, C. R., Delanova, M. O., & Mochamad Yani, Y. (2022). Pengaruh Perang Rusia Dan

Ukraina Terhadap Perekonomian Negara Kawasan Asia Tenggara. *Jurnal Caraka Prabu*, *6*(1), 65–86. https://doi.org/10.36859/jcp.v6i1.1019

Benuf, K., Mahmudah, S., & Priyono, E. A. (2019). Perlindungan Hukum Terhadap Keamanan Data Konsumen Financial Technology Di Indonesia. *Refleksi Hukum: Jurnal Ilmu Hukum*, *3*(2), 145–160. https://doi.org/10.24246/jrh.2019.v3.i2.p145-160

Disemadi, H. S. (2022). Lenses of Legal Research: A Descriptive Essay on Legal Research Methodologies. *Journal of Judicial Review*, *24*(2), 289. https://doi.org/10.37253/jjr.v24i2.7280

Husain, G. S. C. P., Hambali, A. R., & Mappaseleng, N. F. (2020). Indonesia Journal of Criminal Law (IJoCL). *Indonesia Journal of Criminal Law*, *2*(2), 93–104.

Karisma, G. (2023). Keamanan Manusia Di Lampung: Dilema Pemerintah Daerah Dalam Menghadapi Ragam Ancaman Keamanan. *Inovasi Pembangunan –Jurnal Kelitbangan*, *11*(2), 161–176.

Mamluchah, L., & Mubarok, N. (2020). PENCURIAN PADA MASA PANDEMI DALAM TINJAUAN KRIMINOLOGI DAN HUKUM PIDANA ISLAM hidup manusia . Negara-negara yang terjangkit pandemi covid-19 menanggulangi sejumlah efek yang bersifat non medis , khususnya PHK sudah menjad hal yang wajar sejak perusahaan m. *Al-Jinayah*, *6*(1), 1–26. https://jurnalfsh.uinsby.ac.id/index.php/hpi/article/view/1037

Manurung, Y. S. (2024). Konsepsi Kebijakan Strategis Pengelolaan Nikel Di Era Artificial Intelligence Dalam Mendukung Teknologi Kedirgantaraan. *Indonesian Journal of Innovation Multidisipliner Research*, *2*(2), 343–368. https://doi.org/10.69693/ijim.v2i2.141

Sa'diyah, N. K., & Vinata, R. T. (2016). Rekonstruksi Pembentukan National Cyber Defense Sebagai Upaya Mempertahankan Kedaulatan Negara. *Perspektif*, *21*(3), 168. https://doi.org/10.30742/perspektif.v21i3.587

Soewardi, B. A. (2013). Perlunya pembangunan sistem pertahanan siber (Cyber defense) yang tangguh bagi Indonesia. *Potensi Pertahanan*, 31–35.

Umra, S. I. (2019). Penerapan Konsep Bela Negara, Nasionalisme Atau Militerisasi Warga Negara. *Jurnal Lex Renaissance*, *4*(1), 164–178. https://doi.org/10.20885/jlr.vol4.iss1.art9