



Implementasi Keamanan Cyber Berbasis Nilai Nilai Kebangsaan UUD 1945 di Era Digital Best Practice di Perusahaan Pertamina

Thomas Komansilan

Universitas Bhayangkara Jakarta Raya

Edy Soesanto

Universitas Bhayangkara Jakarta Raya

Natasha Salsabillah

Universitas Bhayangkara Jakarta Raya

Alamat: Jl. Raya Perjuangan No 81, RT.003/RW.002, Marga Mulya, Kec. Bekasi Utara, Kota Bks, Jawa Barat 17143

Korespondensi penulis : thomaskomansilan56@gmail.com¹, edy.soesanto@dsn.ubharajaya.ac.id², natashabila04@gmail.com³

Abstract. *The advancement of digital technology has brought about significant progress across various sectors, while simultaneously introducing new risks, particularly in the realm of cybersecurity. Cybersecurity has become a critical concern for companies, including energy giants like Pertamina. In the context of Indonesia, adherence to cybersecurity within Pertamina must align with relevant legal frameworks, such as the 1945 Constitution (UUD 1945). This research aims to explore optimal approaches to implementing cybersecurity within Pertamina, with a focus on the legal underpinnings of the 1945 Constitution. Key attention is directed towards Article 27, paragraph (3) of the Constitution, which guarantees universal access to education, including information security training for employees—a crucial element in thwarting cyber threats. Furthermore, Article 28, paragraph (1) of the 1945 Constitution, safeguarding freedom of association, can be interpreted to endorse collaboration between Pertamina and external entities, like cybersecurity institutions and regulatory bodies, to bolster cyber defense capabilities. Integration of cutting-edge security technology is paramount, aligning with the principles outlined in Article 33, paragraph (2) of the 1945 Constitution, emphasizing the preservation of natural resources. This extends to safeguarding Pertamina's data and digital infrastructure through measures like encryption technology, robust network security protocols, and effective intrusion detection systems. By heeding the legal foundations provided by the 1945 Constitution, the implementation of cybersecurity at Pertamina must be comprehensive, encompassing employee education, technological upgrades, and collaborative efforts with external stakeholders. Such measures aim to mitigate cyber risks, safeguard operational interests, and shield sensitive information from evolving threats in today's digital landscape. Additionally, Law Number 11 of 2008 plays a crucial role in governing information technology and electronic transactions in Indonesia. This legislation grants legal validity to electronic documents, signatures, and transactions, while also ensuring information security and user privacy. It imposes criminal penalties for illicit activities in the realm of information technology, fostering a secure environment for electronic transactions and upholding user rights in the digital age.*

Keywords: : 1945 Constitution, digital era, cyber security, Pertamina, ITE

Abstrak. Perkembangan teknologi digital telah memberikan kontribusi signifikan terhadap kemajuan dalam berbagai bidang, namun juga membawa risiko baru, terutama dalam hal keamanan siber. Kebutuhan akan keamanan cyber telah menjadi sangat penting bagi perusahaan, termasuk perusahaan energi seperti Pertamina. Dalam konteks Indonesia, Implementasi Keamanan Siber dalam Perusahaan Pertamina haruslah sesuai dengan dasar hukum yang berlaku, salah satunya adalah Undang-Undang Dasar 1945 (UUD 1945). Studi ini bertujuan untuk menyelidiki praktik terbaik dalam implementasi keamanan siber di Pertamina, dengan mempertimbangkan kerangka hukum yang diberikan oleh UUD 1945. Salah satu aspek penting yang harus dipertimbangkan adalah Pasal 27 ayat (3) UUD 1945, yang menjamin hak setiap warga negara untuk memperoleh pendidikan dan pengajaran. Dalam konteks keamanan siber, pendidikan dan pelatihan karyawan tentang praktik keamanan informasi menjadi kunci untuk mencegah serangan cyber. Selain itu, Pasal 28 ayat (1) UUD 1945, yang menjamin kebebasan berserikat dan berkumpul secara damai, dapat diinterpretasikan sebagai dukungan untuk kolaborasi antara berbagai entitas dalam mengatasi ancaman keamanan siber. Pertamina dapat mengadopsi praktik kolaboratif dengan pihak eksternal, seperti lembaga penelitian dan keamanan siber, serta pihak berwenang, untuk meningkatkan kemampuan deteksi dan respons terhadap ancaman cyber. Implementasi teknologi keamanan mutakhir juga menjadi fokus utama. Pasal 33 ayat (2) UUD 1945, yang menekankan perlindungan bagi sumber

daya alam, dapat diinterpretasikan dalam konteks perlindungan data dan infrastruktur digital Pertamina. Penerapan teknologi enkripsi, keamanan jaringan yang canggih, dan sistem deteksi intrusi yang efektif merupakan langkah-langkah krusial untuk menjaga keamanan siber perusahaan. Dengan memperhatikan landasan hukum yang diberikan oleh UUD 1945, implementasi keamanan siber di Pertamina haruslah holistik dan melibatkan berbagai aspek, mulai dari pendidikan dan pelatihan karyawan hingga adopsi teknologi keamanan terkini. Dengan demikian, perusahaan dapat meminimalkan risiko serangan siber dan melindungi kepentingan operasional serta informasi sensitif dari ancaman yang terus berkembang di era digital saat ini, dengan dasar UUD 1945 yang berisi Undang-Undang (ITE) Nomor 11 Tahun 2008 adalah undang-undang yang penting dalam mengatur penggunaan teknologi informasi dan transaksi elektronik di Indonesia. Undang-undang (ITE) ini memberikan pengakuan hukum terhadap dokumen, tanda tangan, dan transaksi elektronik, serta memberikan perlindungan terhadap keamanan informasi dan privasi pengguna. Selain itu, Undang-Undang ini juga menetapkan sanksi pidana bagi pelaku tindakan kriminal dalam penggunaan teknologi informasi. Implementasi yang efektif dari Undang-Undang Nomor 11 Tahun 2008 diharapkan dapat meningkatkan keamanan dan kepercayaan dalam melakukan transaksi elektronik serta melindungi hak dan privasi pengguna dalam era digital.

Kata kunci UUD 1945, era digital, keamanan siber, Pertamina, ITE

LATAR BELAKANG

Dalam era digital yang semakin berkembang pesat, tantangan terkait keamanan cyber menjadi semakin kompleks dan mendesak untuk diatasi. Di tengah dinamika tersebut, Indonesia sebagai negara berdasarkan Pancasila dan Undang-Undang Dasar 1945 memiliki komitmen yang kuat terhadap nilai-nilai kebangsaan, termasuk di dalamnya keamanan cyber. Pasal 27 ayat (3), Pasal 28 ayat (1), dan Pasal 33 ayat (2) UUD 1945 menyatakan hak asasi manusia yang harus dilindungi, hak atas privasi, dan kewajiban negara untuk melindungi serta memajukan ilmu pengetahuan dan teknologi bagi kesejahteraan rakyat. Sejalan dengan semangat konstitusi tersebut, Pemerintah Indonesia telah merespons tantangan keamanan cyber dengan mengeluarkan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE). Undang-undang ini memberikan landasan hukum yang kuat untuk melindungi keamanan siber dan mengatur penggunaan teknologi informasi secara aman dan bertanggung jawab. Salah satu entitas yang memiliki peran penting dalam mewujudkan implementasi keamanan cyber berbasis nilai-nilai kebangsaan dan UUD 1945 adalah perusahaan BUMN (Badan Usaha Milik Negara) seperti Pertamina. Sebagai salah satu perusahaan energi terkemuka di Indonesia, Pertamina memiliki tanggung jawab besar dalam menjaga infrastruktur teknologi informasi dan sistemnya dari ancaman siber yang beragam dan terus berkembang. Dalam konteks ini, penting untuk mengidentifikasi dan menerapkan praktik terbaik (best practice) dalam keamanan cyber di Pertamina. Praktik-praktik ini haruslah sejalan dengan nilai-nilai kebangsaan yang tertuang dalam UUD 1945 serta memperhatikan ketentuan-ketentuan yang tercantum dalam ITE Nomor 11 Tahun 2008. Dengan demikian, implementasi keamanan cyber di Pertamina tidak hanya menjadi upaya untuk melindungi aset dan operasional perusahaan, tetapi juga merupakan wujud nyata dari komitmen terhadap nilai-nilai

kebangsaan dan peraturan hukum yang berlaku. Dalam penelitian ini, kami akan menyelidiki praktik terbaik dalam keamanan cyber yang dapat diterapkan di Pertamina, dengan mempertimbangkan nilai-nilai kebangsaan yang diwariskan oleh UUD 1945 serta kerangka hukum yang terkandung dalam ITE Nomor 11 Tahun 2008. Melalui pendekatan ini, diharapkan dapat memberikan kontribusi positif bagi pengembangan strategi keamanan cyber yang efektif dan berkelanjutan dalam menjaga integritas dan kelangsungan operasional Pertamina di era digital ini. Pada titik ini, implementasi keamanan cyber yang berbasis pada nilai-nilai kebangsaan UUD 1945 menjadi Suatu situasi yang memerlukan penyelesaian dan menghadirkan kesulitan yang harus diatasi dengan cermat oleh Perusahaan Pertamina. Dengan memastikan bahwa keamanan cyber mereka tidak hanya mematuhi standar teknis yang tinggi, tetapi juga mencerminkan nilai-nilai kebangsaan yang tercermin dalam UUD 1945, Perusahaan Pertamina dapat memperkuat kedaulatan informasi, melindungi hak-hak asasi manusia, dan meningkatkan ketahanan nasional di era digital yang penuh risiko ini. Dalam konteks inilah, tulisan ini akan mengulas tentang implementasi keamanan cyber berbasis nilai-nilai kebangsaan UUD 1945 di Perusahaan Pertamina. Selain itu, juga akan dibahas praktik terbaik yang dapat diterapkan dalam menjaga keamanan cyber di tengah tantangan dan kompleksitas era digital saat ini. Dengan demikian, tulisan ini diharapkan dapat memberikan wawasan yang mendalam tentang pentingnya mengintegrasikan nilai-nilai kebangsaan dalam strategi keamanan cyber perusahaan, serta memberikan panduan praktis dalam menghadapi ancaman cyber yang semakin canggih di masa depan

METODE PENELITIAN

Metodologi penelitian merupakan landasan yang sangat penting dalam proses penyusunan dan pelaksanaan suatu penelitian. Metodologi ini mencakup serangkaian langkah sistematis yang dirancang untuk mengumpulkan, menganalisis, dan menafsirkan data dengan tujuan menjawab pertanyaan penelitian yang diajukan. Salah satu komponen utama dalam metodologi penelitian adalah desain penelitian yang dipilih, yang mencakup pemilihan teknik pengumpulan data, populasi atau sampel yang diteliti, serta prosedur analisis data yang akan digunakan. Selain itu, metodologi penelitian juga mempertimbangkan aspek-aspek etika dalam penelitian, seperti perlindungan terhadap subjek penelitian dan keabsahan data yang diperoleh. Dengan mengikuti metodologi yang tepat, peneliti dapat memastikan keakuratan dan keandalan hasil penelitian yang dihasilkan serta meningkatkan kontribusi penelitian terhadap pengembangan ilmu pengetahuan. Metode penulisan penelitian ini menggunakan metode studi literatur dan analisa data. Dalam penelitian ini peneliti melakukan observasi dari berbagai studi

kasus maupun sumber sumber yang menjadi landasan dasar mengenai implementasi keamanan cyber berbasis nilai nilai kebangsaan UUD 1945 di era digital best practice di perusahaan pertamanina Penggunaan studi literatur ini bertujuan untuk menjadi pembatas dan perbedaan antara jurnal penulis dengan jurnal lain sehingga tidak terjadi plagiarisme atau cetak copyright dari penulis jurnal lainnya. Manfaat dari penelitian studi literatur ini untuk mengetahui tingkat keamanan suatu sistem produksi dan faktor yang mempengaruhi suatu sistem produksi dengan UUD 1945. Dengan mengetahui aspek yang mempengaruhi produksi suatu industri, maka manajemen perusahaan dapat menetapkan segi aturan maupun tata tertib dan menganalisis semua kemungkinan yang terjadi selama proses industri agar manajemen perusahaan dapat mengambil tindakan pencegahan. Pembuatan metode penulisan ini menjadi acuan untuk membedakan titik kemiripan dan titik perbedaan suatu karya penulis agar tidak menjadi Hak Copyright dan memastikan penulis tidak melakukan pelanggaran Hak Cipta.

no	Judul jurnal/paper	Penulis /author	Titik kesamaan	Titik perbedaan
1	W.Setiawan, Pengantar Teknologi Informasi, UPI Press, 2011.	W.Setiawan, Pengantar Teknologi Informasi, UPI Press, 2011.	Perkembangan teknologi digital telah memberikan kontribusi signifikan terhadap kemajuan dalam berbagai bidang, namun juga membawa risiko baru	Terdapat perbedaan Era digital harus disikapi dengan serius, menguasai, dan mengendalikan peran teknologi dengan baik agar era digital membawa manfaat bagi kehidupan.
2	Asril Sitompul membahas tentang Hukum Internet dalam bukunya yang berjudul "Pengenalan Mengenai Masalah Hukum di Cyberspace," yang diterbitkan oleh Citra Aditya pada tahun 2001.	t. Asril Sitompul. Hukum Internet (Pengenalan Mengenai Masalah hukum di Cyberspace, (Bandung: Citra Aditya, 2001).	Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) yang diterbitkan dalam Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58 mengatur tentang	UU ini menyediakan dasar hukum yang solid untuk memperkuat perlindungan terhadap keamanan siber serta mengatur penggunaan teknologi informasi dengan cara yang aman.

			teknologi informasi yang sangat bermanfaat.	
3.	Kajian hukum terkait penanganan cyber crime di indonesia	Salma elsa anidya, universitas pembangunan nasional (2023)	Menjelaskan hukum-hukum cyber sekuriti lebih terinci tentang UU ITE	Menggunakan UU ITE sebagai salah satu konteks dalam cyber sekuriti
	Suharyanto, Budi. 2013. Tindak Pidana Teknologi Informasi	Suharyanto,budi.2013	Tentang permasalahan penerobosan web secara paksa yang dilakukan tanpa izin	Membahas tentang keamana cyber sekuriti dalam konteks keamana data.dalam Perusahaan pertamina
4.	Cybercrime: pemahaman dan upaya penjegahan kejahatan berteknologi.	Raharjo, Agus. 2002	Pelanggaran terhadap keamanan sistem dan data komputer, yang meliputi integritas, ketersediaan, dan kerahasiaan, seperti tindakan hacking, cracking, atau trespass komputer, adalah upaya untuk secara ilegal masuk, mengubah, atau merusak sistem atau data komputer tanpa izin yang sah.	implementasi keamanan cyber di Pertamina tidak hanya menjadi upaya untuk melindungi aset dan operasional perusahaan,
5	Widodo. 2009. Sistem Pidana dalam Cyber Crime	Widodo. 2009.	Transaksi elektronik mengatu pula tentang akses computer atau	Menjelaskan Undang-undang (ITE) ini memberikan pengakuan

			<p>system electronic dengan cara apapun mengakses komputer atau system dengan cara apapun</p>	<p>hukum terhadap dokumen, tanda tangan, dan transaksi elektronik, serta memberikan perlindungan terhadap keamanan informasi dan privasi pengguna. Selain itu, Undang-Undang ini juga menetapkan sanksi pidana bagi pelaku tindakan kriminal dalam penggunaan</p>
6	Humaira Aliya, Kupas Tuntas Cybersecurity.	Humaira Aliya	<p>Di zaman digital ini, keamanan cyber menjadi kebutuhan yang sangat penting bagi individu maupun entitas bisnis.</p> <p>Glints telah menyusun informasi mengenai konsep dan kegunaan dari keamanan cyber.</p>	<p>Perkembangan teknologi digital telah memberikan kontribusi signifikan terhadap kemajuan dalam berbagai bidang, namun juga membawa risiko baru, terutama dalam hal keamanan siber.</p> <p>Kebutuhan akan keamanan cyber telah menjadi sangat penting bagi perusahaan, termasuk perusahaan energi seperti Pertamina.</p>

7	Opini tentang pentingnya undang-undang keamanan dan ketahanan di ranah siber yang disampaikan oleh Kurniawan dan Galih Eko pada tahun 2019."	Kurniawan,Galih Eko. (2019)	Menjelaskan kemaana siber ,pemulihan, ,berdasarkan UU ITE	Tindakan untuk menangani, memulihkan, memantau, dan mengendalikan objek-objek terkait keamanan siber.
8	Artikel yang Anda sebutkan berjudul "Analisis Risiko dan Keamanan Informasi pada Sebuah Perusahaan System Integrator Menggunakan Metode Octave Allegro" oleh Deva, B. S., & Jayadi, R. (2022), yang diterbitkan dalam Jurnal Teknologi dan Informasi (JATI), Volume 12, Nomor 2.	Deva, B. S., & Jayadi, R. (2022)	Organisasi harus menerapkan audit manajemen keamanan informasi yang disesuaikan dengan persyaratan yang berlaku untuk melindungi perusahaan	Artikel ini membahas tentang kemaan data dan informasi dengan Upaya menjaga kemungkinnya kehilangan data
9	"Information Security Management System (ISMS) Menggunakan Standar ISO/IEC 27001:2005" oleh Syafrizal, M. (2009).	Syafrizal, M. (2009).	Berdasarkan pembahsan masalah penelitian beresiko terhadap keamanan informasi	Jurnal ini memliki pemabahsan yang hampirr mirip sama sama membahasa dan meneliti keamanan Informasi
10	, Cyber War: The Challenge to National Security, Global Security Studies, Winter 2013, Volume 4, Issue 1, University of North Carolina Wilmington	Nathalie Chaplan	Jurnal ini menceritakan tentang seluk beluk uud kemana siber secara menyeluruh	Jurnal ini sedikit memliki kesamaan menjelaskan uud tentang keamanan siber tetapi tidak secara detail
11	Cyber Crime dalam Bentuk Phising Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik	Ardi Saputra Gulo, Sahuri Lasmadi, Kabib Nawawi	Artikel ini menjelaskan tentang kasus-kasus yang sering terjadii di	Juranl ini menjelaskan dengan berbading terballik dengan

			dunia cyber seperti phising Ddos, pencurian data	artikel tersebut Dimana jurnal ini menjelaskan cara untuk mencegah kasus kasus yang terjadi di dunia cyber .
12	pengaruh auditor internal dan kebijakan manajemen terhadap efektivitas keamanan siber	Sherina deni darwanti	Artikel ini menjelaskan tentang bahayanya suatu perusahaan tidak mengetahui bahayanya efektivitas siber pada perusahaannya	Jurnal ini menjelaskan bahwa tentang sebab dan akibat , dan kerugian yang di timbulkan olehh efektivitas siberr pada suatu siber bila tidak ada pencegahannya
13	Implications of Defense Diplomacy on Cybersecurity in Context Security Politics	Lazuardi Loqman Ar Rahman	Konsep keamanan nasional membahas bagaimana aktor politik keamanan mengambil langkah-langkah menggunakan berbagai strategi yang tersedia dalam upaya untuk memenuhi tanggung jawab mereka dalam memberikan perlindungan bagi negara dan warganya di bidang keamanan siber.	Jurnal ini menjelaskan bagaimana cara mencegah pencurian data pada perusahaan yang berbasiis UUD, UU ITE 1945.
14	Pengkajian kejahatan di dunia maya dalam konteks	IS Bahri - 2023	Artike ini menjelaskan	Jurnal ini membahas

	hukum pidana (Edisi tahun 2023)."		tentang konsep konsep siber crime yang landasi dengan hukum pidanan.	tentang mengatasi kejahatan siber yang sedang marak dengan dilandasi hukum.
--	-----------------------------------	--	--	---

15	PENGETAHUAN DASAR IDENTIFIKASI DINI DETEKSI SERANGAN KEJAHATAN SIBER UNTUK MENCEGAH PEMBOBOLAN DATA PERUSAHAAN	TriGinanjjar Laksana,Sri Mulyan	Jurnal ini menjelaskan praktik terbaik yang dapat membantu dalam menghadapi serangan kejahatan siber: membangun strategi dan mengambil tindakan proaktif. Pertama, amankan jaringan internet Anda dengan menggunakan enkripsi dan kata sandi yang kuat.	Jurnal ini mempunyai kesamaan yang sama untuk mencegah terjadinya kejahatan siber yang sering terjadi pada suatu perusahaan contohnya Pertamina
----	--	---------------------------------	---	---

Penelitian ini bertujuan untuk menyelidiki praktik terbaik (best practice) dalam implementasi keamanan cyber yang didasarkan pada nilai-nilai kebangsaan yang terdapat dalam UUD 1945 di era digital, dengan fokus pada perusahaan Pertamina sebagai studi kasus. Keamanan cyber menjadi semakin penting dalam menghadapi tantangan digital di era saat ini, di mana serangan cyber dapat mengancam keberlangsungan operasional dan kepentingan nasional suatu negara.

Metode penelitian yang digunakan meliputi analisis dokumen dan wawancara dengan para ahli keamanan cyber serta pemangku kepentingan terkait di perusahaan Pertamina. Analisis dilakukan untuk mengidentifikasi strategi, kebijakan, dan praktik terbaik yang telah diimplementasikan, serta untuk mengevaluasi sejauh mana nilai-nilai kebangsaan UUD 1945 telah diintegrasikan dalam upaya keamanan cyber perusahaan Pertamina.

Hasil penelitian diharapkan dapat memberikan wawasan yang mendalam tentang bagaimana implementasi keamanan cyber yang berbasis pada nilai-nilai kebangsaan dapat dilaksanakan secara efektif di perusahaan Pertamina, serta memberikan kontribusi pada pemahaman lebih lanjut tentang pentingnya integrasi nilai-nilai kebangsaan dalam strategi keamanan cyber di era digital saat ini.

HASIL DAN PEMBAHASAN

HIPOTESA IMPLEMENTASI KEAMANAN CYBER BERBASIS NILAI NILAI KEBANGSAAN UUD 1945 DI ERA DIGITAL BEST PRACTICE DI PERUSAHAAN PERTAMINA.

NO	Hasil perbedaan	Hipotesa	Analisa
Z1	<ul style="list-style-type: none"> • Dalam rangka Tentang kemajuan cyber dalam era digital • Transformasi sosial ekonomi dan politik di seluruh dunia yang perlu di analisis dalam kontek kemajuan cyber dalam era digital 	P1:UUD 1945	Z1-P1 UU No. 11 Tahun 2008, yang telah diubah dengan UU No. 19 Tahun 2016. UU ITE mencakup ketentuan mengenai transaksi elektronik, sistem informasi, UU No. 27 Tahun 2022, Peraturan Pemerintah No. 71 Tahun 2019, yang merupakan perubahan dari PP No. 82 Tahun 2012. didalam peraturan ini mengenai perkembangan cyber crime.
Z2	<ul style="list-style-type: none"> • tentang Informasi dan Transaksi Elektronik (selanjutnya disingkat UU ITE) dalam Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58. Teknologi informasi sangat bermanfaat.. • meskipun uu ITE memiliki tujuan yang baik untuk 	P2: UUD 1945	Z2-P2 Beberapa pasal dalam UU ITE, terutama pasal yang berkaitan dengan pencemaran nama baik (Pasal 27 ayat 3), sering dikritik karena dianggap "pasal karet" yang bisa ditafsirkan secara luas dan

	<p>mengatur penggunaan teknologi informasi dan transaksi elektronik implementasinya juga banyak menimbulkan berbagai kontroversi</p> <ul style="list-style-type: none"> • pasal uu tersebut telah digunakan untuk menekan kebebasan berbicara dan berekspresi di sosial media yang mencakup platform daring lainnya. 		<p>digunakan untuk membungkam kritik. Kebebasan Berpendapat: Banyak aktivis dan organisasi masyarakat sipil mengkritik UU ITE karena potensial membatasi kebebasan berpendapat di internet. Perubahan dan Revisi Ada desakan dari berbagai kelompok masyarakat untuk merevisi UU ITE, terutama untuk memperjelas beberapa pasal yang dianggap ambigu dan membatasi kebebasan sipil. Diskusi mengenai revisi ini terus berlangsung, dengan harapan dapat menciptakan keseimbangan antara keamanan siber dan kebebasan berpendapat.</p> <p>Secara keseluruhan, UU ITE adalah batu penjur dalam kerangka hukum digital Indonesia, tetapi masih memerlukan beberapa perbaikan untuk menyesuaikan dengan perkembangan teknologi dan norma sosial yang terus berubah.</p>
Z3	<ul style="list-style-type: none"> • implementasi keamanan cyber di Pertamina tidak hanya menjadi upaya untuk melindungi aset dan operasional perusahaan, 	.	<p>Z3-p3 Undang-Undang No. 40 Tahun 2007 tentang Perseroan Terbatas (UU PT): UU ini mengatur tentang pendirian, pengelolaan, dan tanggung jawab</p>

	<ul style="list-style-type: none"> • Langkah penting ini juga untuk menjaga reputasi dan nama baik perusahaan • Dan Perusahaan juga memastikan kelangsungan bisnis dan beberapa analisis terkait implementasi keamanan cyber. 	<p>P3: UUD 1945</p>	<p>perseroan terbatas. Meskipun fokus utamanya bukan pada pencemaran nama baik, UU ini mencakup aspek-aspek perlindungan hukum terhadap aset perusahaan, termasuk reputasi. Undang-Undang No. 30 Tahun 2000, Undang-Undang No. 8 Tahun 1999 tentang Perlindungan Konsumen, Undang-Undang Informasi dan Transaksi Elektronik (UU ITE): Seperti yang telah disebutkan sebelumnya, UU ITE (Undang-Undang No. 11 Tahun 2008) Undang-Undang ini terkait dengan menjaga nama baik konsumen dan aset operasional Perusahaan.</p>
Z4	<ul style="list-style-type: none"> • Dampak dan kerugian yang dihasilkan dari ke kurangnya pengetahuan tentang cyber sekuriti, dalam UUD 1945 mulai dari penjangkan dalam keamanan datanya dalam masing-masing Perusahaan. • Tidak ada nya best practice terhadap karyawan tentang pengetahuan cyber crime • Perlindungan data -data aset operasional Perusahaan dan data-data pribadi mili karyawan dalam perusahaan. 	<p>P4: UUD 1945</p>	<p>Z4-p4 Undang-Undang Nomor 40 Tahun 2007 tentang Perseroan Terbatas (UU PT) adalah peraturan yang mengatur beragam aspek operasional dan hukum yang terkait dengan badan hukum perusahaan yang disebut perseroan terbatas., termasuk tanggung jawab hukum dan bagaimana kerugian yang dialami oleh perusahaan harus ditangani, terutama dalam hal pertanggungjawaban direksi dan dewan komisaris, Undang-Undang No. 30 Tahun</p>

			2000, Undang-Undang No. 8 Tahun 1999 tentang Perlindungan Konsumen, Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi, Undang-Undang No. 13 Tahun 2003 tentang Ketenagakerjaan, setiap kerugian yang dialami oleh perusahaan harus dianalisis berdasarkan konteks spesifik dari kerugian tersebut dan undang-undang yang relevan.
--	--	--	---

KESIMPULAN DAN SARAN

Era digital yang semakin berkembang pesat membawa tantangan yang semakin kompleks dalam hal keamanan cyber. Serangan cyber menjadi lebih beragam dan terus berkembang, memerlukan respons yang cepat dan efektif dari entitas-entitas yang terlibat. Sebagai negara berdasarkan Pancasila dan UUD 1945, Indonesia memiliki komitmen yang kuat terhadap nilai-nilai kebangsaan, termasuk keamanan cyber. Hal ini tercermin dalam Pasal 27 ayat (3), Pasal 28 ayat (1), dan Pasal 33 ayat (2) UUD 1945 yang menegaskan hak asasi manusia, hak atas privasi, dan kewajiban negara untuk melindungi serta memajukan ilmu pengetahuan dan teknologi. Perusahaan BUMN seperti Pertamina memiliki peran penting dalam mewujudkan implementasi keamanan cyber yang berbasis pada nilai-nilai kebangsaan. Sebagai salah satu perusahaan energi terkemuka di Indonesia, Pertamina memiliki tanggung jawab besar dalam menjaga infrastruktur teknologi informasi dan sistemnya dari ancaman siber yang beragam. Implementasi keamanan cyber di Pertamina harus memperhatikan praktik terbaik yang sejalan dengan nilai-nilai kebangsaan yang diwariskan oleh UUD 1945 serta memperhatikan ketentuan-ketentuan dalam ITE Nomor 11 Tahun 2008. Hal ini tidak hanya untuk melindungi aset dan operasional perusahaan, tetapi juga sebagai wujud nyata dari komitmen terhadap nilai-nilai kebangsaan dan peraturan hukum yang berlaku. Implementasi keamanan cyber yang berbasis pada nilai-nilai kebangsaan UUD 1945 merupakan tantangan yang harus dihadapi dengan cermat oleh Perusahaan Pertamina. Namun, dengan memastikan bahwa keamanan cyber mereka mencerminkan nilai-nilai kebangsaan, Pertamina dapat memperkuat kedaulatan

informasi, melindungi hak-hak asasi manusia, dan meningkatkan ketahanan nasional di era digital.

DAFTAR REFERENSI

- 13.+*Jurnal+JUKIM+Tri+Ginanjari+Laksana*. (n.d.).
- Ar rahman, L. L. (2021). Implikasi Diplomasi Pertahanan terhadap Keamanan Siber dalam Konteks Politik Keamanan. *Jurnal Diplomasi Pertahanan*, 6(2). <https://doi.org/10.33172/jdp.v6i2.654>
- Budi, E., Wira, D., & Infantono, A. (2021). Strategi Penguatan Cyber Security Guna Mewujudkan Keamanan Nasional di Era Society 5.0. *Prosiding Seminar Nasional Sains Teknologi Dan Inovasi Indonesia (SENASTINDO)*, 3(November), 223–234. <https://doi.org/10.54706/senastindo.v3.2021.141>
- Fachrudin, R., Respaty, E., Adilah, I. S., & ... (2024). Peranan Penting Manajemen Sekuriti di Era Digitalisasi. *Nusantara Journal of ...*, 2(1), 94–102. <https://jurnal.intekom.id/index.php/njms/article/view/252>
- Gulo, A. S., Lasmadi, S., & Nawawi, K. (2021). Cyber Crime dalam Bentuk Phising Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik. *PAMPAS: Journal of Criminal Law*, 1(2), 68–81. <https://doi.org/10.22437/pampas.v1i2.9574>
- Hukum Dan Regulasi Ict Terhadap Cyber Cr.* (n.d.).
- Nadjiha, S. (2019). Japs 1. *Jurnal Asia Pacific Studies*, 4 Number 1(1), 33–45. <https://dx.doi.org/10.33541/japs.v4i1.1640>
- Nainggolan, N. S., & Nasution, I. P. (2023). Pentingnya Keamanan Big Data Dalam Lembaga Pemerintahan Di Era Digital. *Jurnal Sains Dan Teknologi (JSIT)*, 3(2), 253–257. <https://doi.org/10.47233/jsit.v3i2.883>
- Nugraha, R. (2021). Perspektif Hukum Indonesia (Cyberlaw) Penanganan Kasus Cyber di Indonesia. *Jurnal Ilmiah Hukum Dirgantara*, 11(2), 44–56.
- Romadhan, R. C. (2021). Kedudukan Hukum Badan Usaha Milik Negara Sebagai Anak Perusahaan Dalam Perusahaan Holding Induk. *Media Iuris*, 4(1), 73. <https://doi.org/10.20473/mi.v4i1.23669>
- Safitri, R. (2018). Undang-Undang Informasi dan Transaksi Elektronik Bagi Perguruan Tinggi. *SALAM: Jurnal Sosial Dan Budaya Syar-I*, 5(3), 197–218. <https://doi.org/10.15408/sjsbs.v5i3.10279>
- Sherina, & Darmawati, D. (2022). Pengaruh Auditor Internal dan Kebijakan Manajemen Terhadap Efektivitas Keamanan Siber. *Jurnal Ekonomi Trisakti*, 2(2), 515–528. <https://www.trijurnal.trisakti.ac.id/index.php/jet>
- Silalahi, F. D. (2022). Keamanan Cyber (Cyber Security). *Penerbit Yayasan Prima Agus Teknik*, 1–285. <http://penerbit.stekom.ac.id/index.php/yayasanpat/article/view/367>
- Soesanto, E., & Wijayanti, A. (2023). *Cross-border MENGELOLA OBJEK VITAL, PENGAMANAN FILE, DAN PENGAMANAN CYBER TERHADAP MANAJEMEN SEKURITI PADA PT. PERTAMINA (PERSERO)*. 6(1), 670–679.
- (Ar rahman, 2021)(13.+*Jurnal+JUKIM+Tri+Ginanjari+Laksana*, n.d.)(Gulo et al., 2021)(Fachrudin et al., 2024)(Soesanto & Wijayanti, 2023)(Silalahi, 2022)(Budi et al.,

2021)(Nugraha, 2021)(*Hukum_Dan_Regulasi_Ict_Terhadap_Cyber_Cr*, n.d.)(Nainggolan & Nasution, 2023)(Safitri, 2018)(Romadhan, 2021)(Romadhan, 2021)

Safitri, R. (2018). Artikel yang membahas tentang penerapan Undang-Undang Informasi dan Transaksi Elektronik di lingkungan perguruan tinggi.. *SALAM: Jurnal Sosial Dan Budaya Syar-I*, 5(3), 197–218. <https://doi.org/10.15408/sjsbs.v5i3.10279>

(Nadjih, 2019)