Konstitusi : Jurnal Hukum, Administrasi Publik, dan Ilmu Komunikasi
Volume. 3 Nomor. 1 Januari 2026
E-ISSN : 3063-4040; P-ISSN : 3063-3877, Hal 118-128
DOI: https://doi.org/10.62383/konstitusi.v3i1.1514
Tersedia: https://ejournal.appihi.or.id/index.php/Konstitusi

Kesiapan Regulasi Hukum Siber di Indonesia dalam Menghadapi Ancaman Global

(Studi Banding dengan Uni Eropa dan Amerika Serikat)

Muhammad Taufik Rusydi[1*], Gesang Kristianto Nugrohotomo[2]
[1, 2] Teknik Informatika, Fakultas Teknik Elektro dan Informatika, Universitas Surakarta, Indonesia
**Penulis Korespondensi: mtaufikrusydi@gmail.com*

Abstract. *In the increasingly developing digital era, cyber law regulation has become a crucial element in maintaining security and order in cyberspace. Indonesia, as a country with rapid technological growth, faces major challenges in responding to global threats in the cyber sector. This study aims to analyze the readiness of cyber law regulation in Indonesia by comparing it to the regulations implemented in the European Union and the United States. A qualitative approach is used with descriptive and normative analysis methods to examine the applicable cyber law policies. The results of the study show that Indonesia still has many limitations in cyber law enforcement, especially in terms of data protection, cybercrime, and coordination mechanisms between related institutions. On the other hand, the European Union already has a comprehensive General Data Protection Regulation (GDPR), while the United States applies a sectoral approach with different regulations in each field. This study suggests the need for regulatory reform that is more adaptive and responsive to global threats, as well as increased international cooperation in cyber law enforcement. Thus, Indonesia can be better prepared to face increasingly complex cyber challenges.*

Keywords*: Cyber Law; Cyber Security; Global Threats; Personal Data Protection; Regulation.*

Abstrak. Di era digital yang semakin berkembang, regulasi hukum siber telah menjadi elemen penting dalam menjaga keamanan dan ketertiban di dunia maya. Indonesia, sebagai negara dengan pertumbuhan teknologi yang pesat, menghadapi tantangan besar dalam menanggapi ancaman global di sektor siber. Studi ini bertujuan untuk menganalisis kesiapan regulasi hukum siber di Indonesia dengan membandingkannya dengan regulasi yang diterapkan di Uni Eropa dan Amerika Serikat. Pendekatan kualitatif digunakan dengan metode analisis deskriptif dan normatif untuk menguji kebijakan hukum siber yang berlaku. Hasil penelitian menunjukkan bahwa Indonesia masih memiliki banyak keterbatasan dalam penegakan hukum siber, terutama dalam hal perlindungan data, kejahatan siber, dan mekanisme koordinasi antar lembaga terkait. Di sisi lain, Uni Eropa telah memiliki Peraturan Perlindungan Data Umum (GDPR) yang komprehensif, sementara Amerika Serikat menerapkan pendekatan sektoral dengan regulasi yang berbeda di setiap bidang. Studi ini menyarankan perlunya reformasi regulasi yang lebih adaptif dan responsif terhadap ancaman global, serta peningkatan kerja sama internasional dalam penegakan hukum siber. Dengan demikian, Indonesia dapat lebih siap menghadapi tantangan siber yang semakin kompleks.

Kata kunci: Ancaman Global; Hukum Siber; Keamanan Siber; Perlindungan Data Pribadi; Regulasi.

1. LATAR BELAKANG

Dalam beberapa dekade ini, majunya teknologi informasi dan komunikasi telah menghadirkan perubahan yang besar ke dalam berbagai aspek kehidupan manusia, bahkan pada bidang hukum dan keamanan di dunia digital. Dunia maya yang semakin maju dengan kehidupan sehari-hari memperluas peluang dan menciptakan tantangan baru, seperti kejahatan siber, perlindungan data, atau regulasi-peraturan digital. Negara-negara di seluruh dunia, termasuk Indonesia, dalam menghadapi berbagai tantangan untuk memastikan rancangan regulasi hukum siber mereka mampu disesuaikan untuk mengatasi ancaman global yang semakin komplek(Solms & Niekerk, 2013). Regulasi hukum Siber di Indonesia berhadapan dengan masih banyak permasalahan yang termanifestasikan dalam aspek penetapan kebijakan, penegakan, koordinasi antara lembaga penegak norma positif yang dipanggil untuk

Artikel Masuk: 26 November 2025; Revisi: 30 Desember 2025; Diterima: 25 Januari 2025; Terbit: 30 Januari 2026

melaksanakan tugas terkait keamanan siber. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) beserta perubahannya dalam Undang-Undang Nomor 19 Tahun 2016 yang menjadi hukum utama penyelenggaraan kegiatan digital di Indonesia. Lagipula, regulasi ini masih memiliki kelemahan, khususnya dalam menghadapi ancaman global yang terus membesar (Setyowati, 2021). Pada saat ini Uni Eropa telah menetepkan *General Data Protection Regulation* (GDPR) sebagai peraturan utamanya untuk perlindungan data personal dan keamanan siber. GDPR dicatat sebagai aturan yang sangat ketat dalam melindungi privasi warga negara dan memberikan sanksi terhadap perusahaan organisasi melanggar aturan perlindungan data (Union, 2018). Di lain sisi Amerika Serikat mengadopsi pendekatan sektoral dalam regulasi hukum siber, putusan perlindungan dan keamanan siber yang berbeda-berbeda sesuai dengan sektor industri. Data yang dikumpulkan selalu menjadi hak cipta pemiliknya (*data owner*). Dikemukakan bahwa perlindungan data telah diatur oleh berbagai bentuk hukum di berbagai negara, contohnya *Health Insurance Portability and Accountability Act* (HIPAA) mengatur pengamanan data kesehatan, sedangkan *Children's Online Privacy Protection Act* (COPPA) mengatur pengamanan kumpulan data anak-anak melalui Internet (Schwartz & Solove, 2011).

Jika dibandingkan dengan Uni Eropa dan Amerika Serikat, regulasi hukum siber di Indonesia masih perlu diperkuat dalam banyak aspek. Salah satu kendala utama yang dihadapi adalah tidak adanya regulasi khusus yang sebanding dengan GDPR untuk perlindungan data pribadi. Sedangkan penegakan hukum terkait kejahatan siber di Indonesia masih mengalami hambatan, baik dari segi sumber daya manusia, teknologi, maupun kerjasama internasional (Kusuma & Wibisono, 2022). Sejalan dengan itu, penelitian ini bertujuan untuk mengevaluasi kesiapan regulasi hukum siber di Indonesia dalam menghadapi ancaman global dengan melakukan perbandingan terhadap regulasi yang diterapkan di Uni Eropa dan Amerika Serikat. Dengan mengenal kelebihan dan kekurangan dari setiap sistem regulasi, diharapkan Indonesia mampu menciptakan regulasi yang lebih fleksibel dan tanggap terhadap perubahan ancaman siber global. Penelitian ini juga akan mengkaji urgensi kolaborasi internasional di sektor keamanan siber untuk memperkuat ketahanan digital negara.

2. KAJIAN TEORITIS

Hukum Siber

Hukum siber (*cyber law*) merupakan seperangkat norma hukum yang mengatur pemanfaatan teknologi informasi dan komunikasi, termasuk aktivitas di internet, transaksi elektronik, serta perlindungan terhadap sistem dan data digital. Hukum siber lahir sebagai

respons atas berkembangnya ruang siber yang bersifat lintas batas negara, sehingga menimbulkan tantangan baru bagi sistem hukum nasional (Setyowati, 2021).

Menurut Marzuki (2017) perkembangan hukum siber menunjukkan adanya pergeseran paradigma hukum dari pendekatan teritorial menuju pendekatan fungsional yang menyesuaikan karakter teknologi informasi (Marzuki, 2017). Ruang lingkup hukum siber meliputi perlindungan data pribadi, kejahatan siber, keamanan sistem elektronik, tanggung jawab penyelenggara sistem elektronik, serta kerja sama internasional dalam penegakan hukum siber (Wijaya, 2021). Dalam konteks Indonesia hukum siber berfungsi sebagai instrumen pengaturan sekaligus perlindungan hukum bagi masyarakat digital. Namun efektivitas hukum siber sangat dipengaruhi oleh kesiapan regulasi, kapasitas institusi, dan koordinasi antarpenegak hukum (Kusuma & Wibisono, 2022).

Perlindungan Data Pribadi

Perlindungan data pribadi merupakan bagian penting dari hak privasi yang melekat pada setiap individu. Secara teoritis, data pribadi dipandang sebagai aset yang harus dikelola secara aman dan bertanggung jawab untuk mencegah penyalahgunaan yang dapat merugikan subjek data (Putri, 2023).

Firmansyah (2020) menjelaskan bahwa perlindungan data pribadi bertujuan untuk menjamin kendali individu atas data pribadinya, termasuk hak untuk mengetahui, mengakses, memperbaiki, dan menghapus data. Prinsip-prinsip perlindungan data pribadi umumnya mencakup legalitas, transparansi, pembatasan tujuan, keamanan data, dan akuntabilitas pengendali data (Firmansyah, 2020a).

Di Indonesia penguatan perlindungan data pribadi ditandai dengan disahkannya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Namun, beberapa kajian menyebutkan bahwa tantangan utama terletak pada implementasi dan penegakan hukum, terutama terkait kelembagaan pengawas dan sanksi administratif (Putri, 2023; Setyowati, 2021).

Kejahatan Siber

Kejahatan siber (*cybercrime*) didefinisikan sebagai segala bentuk perbuatan melawan hukum yang menggunakan sistem elektronik sebagai sarana maupun sasaran tindak pidana. Kejahatan siber memiliki karakteristik khusus, seperti bersifat transnasional, sulit dilacak, serta berdampak luas dalam waktu singkat (Siregar & Hidayat, 2023). Menurut Kusuma dan Wibisono (2022), kejahatan siber di Indonesia masih menghadapi kendala dalam aspek pembuktian, keterbatasan sumber daya manusia, serta kurangnya pemahaman teknis aparat penegak hukum. Oleh karena itu, pendekatan keamanan siber tidak hanya menitikberatkan

pada aspek represif, tetapi juga preventif melalui penguatan sistem, regulasi, dan literasi digital masyarakat (Kusuma & Wibisono, 2022).

Penelitian Terdahulu yang Relevan

Penelitian terdahulu menunjukkan bahwa regulasi hukum siber di Indonesia masih memiliki kelemahan dalam aspek implementasi dan koordinasi. Firmansyah (2020) menemukan bahwa regulasi perlindungan data pribadi di Indonesia belum memiliki mekanisme pengawasan yang kuat (Firmansyah, 2020). Penelitian Kusuma dan Wibisono (2022) menyoroti rendahnya efektivitas penegakan hukum terhadap kejahatan siber akibat keterbatasan sumber daya dan teknologi (Kusuma & Wibisono, 2022).

Setyowati (2021) dalam kajiannya menyatakan bahwa Indonesia perlu melakukan reformasi hukum siber agar lebih selaras dengan standar global. Sementara itu, Putri (2023) menekankan pentingnya penguatan kelembagaan dan kesadaran hukum masyarakat untuk mendukung keberhasilan implementasi UU PDP (Setyowati, 2021).

3. METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif dengan metode analisis deskriptif dan normatif. Pendekatan deskriptif bertujuan untuk menggambarkan dan menganalisis kondisi regulasi hukum siber di Indonesia dalam menghadapi ancaman global dengan membandingkannya terhadap regulasi di Uni Eropa dan Amerika Serikat. Analisis normatif dilakukan dengan menelaah peraturan perundang-undangan yang berkaitan dengan hukum siber di Indonesia serta standar internasional yang diterapkan di Uni Eropa dan Amerika Serikat. Sumber data yang digunakan meliputi dokumen hukum, jurnal akademik, serta kebijakan pemerintah terkait hukum siber. Teknik pengumpulan data dilakukan melalui studi kepustakaan dan analisis dokumen hukum yang relevan. Hasil analisis kemudian dibandingkan secara sistematis untuk mengidentifikasi kesenjangan regulasi dan tantangan implementasi di Indonesia.

4. HASIL DAN PEMBAHASAN

Kesiapan Regulasi Hukum Siber di Indonesia

Regulasi hukum siber di Indonesia masih dalam proses pengembangan dan menghadapi berbagai tantangan dalam pelaksanaannya. Salah satu elemen penting dalam regulasi hukum siber adalah perlindungan data pribadi, yang saat ini diatur melalui Undang-Undang No. 27 Tahun 2022 mengenai Perlindungan Data Pribadi (UU PDP). Walaupun regulasi ini adalah

kemajuan dalam perlindungan data, masih ada kelemahan dalam sistem penegakan hukum dan hukuman bagi para pelanggar (Putri, 2023).

Dalam bidang kejahatan siber Indonesia telah memiliki Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) yang berfungsi sebagai dasar hukum untuk menangani berbagai tindak pidana siber. Namun UU ITE kerap dikecam karena pelaksanaannya yang masih dapat ditafsirkan secara beragam dan berpotensi menimbulkan tindakan kriminal terhadap kebebasan berekspresi (Pratama & Suhendar, 2022).

Dari sudut pandang kolaborasi internasional Indonesia telah turut serta dalam beberapa forum global seperti Kerja Sama Keamanan Siber ASEAN dan berkolaborasi dengan Interpol untuk memerangi kejahatan siber antarnegara. Namun masih diperlukan harmonisasi peraturan dengan norma internasional seperti Konvensi Budapest tentang Kejahatan Siber yang sampai saat ini belum diratifikasi oleh Indonesia (Wijaya, 2021).

Selain itu perbandingan dengan peraturan Uni Eropa menunjukkan bahwa GDPR menawarkan perlindungan data yang lebih ketat dengan prinsip-prinsip yang tegas dalam pengelolaan data. Sedangkan di Amerika Serikat peraturan hukum siber cenderung sektoral dengan adanya undang-undang seperti *California Consumer Privacy Act* (CCPA) yang mengelola perlindungan data pribadi untuk penduduk California. Model regulasi ini menawarkan keluwesan untuk beberapa sektor, tetapi juga menimbulkan tantangan dalam konsistensi hukum siber di tingkat nasional (Nugroho, 2023).

Dalam menghadapi ancaman global Indonesia harus memperbaiki kesiapan regulasi hukum siber dengan mengimplementasikan pendekatan yang lebih menyeluruh dan responsif. Tindakan yang bisa dilakukan meliputi perbaikan UU PDP, perubahan pada UU ITE untuk mencegah penyalahgunaan dan peningkatan kemampuan aparat penegak hukum dalam menangani kasus kejahatan siber (Siregar & Hidayat, 2023). Peraturan hukum siber di Indonesia bisa lebih efisien dalam menghadapi tantangan global dan memberikan perlindungan yang lebih baik untuk masyarakat digital.

Regulasi Hukum Siber di Uni Eropa

Uni Eropa telah mengeluarkan beragam regulasi yang mengatur keamanan dan privasi siber dengan *General Data Protection Regulation* (GDPR) sebagai fondasi utama dalam perlindungan data pribadi. GDPR yang diimplementasikan pada Mei 2018, bertujuan untuk memperkuat perlindungan terhadap data pribadi warga Uni Eropa dan meningkatkan transparansi dalam pengolahan data oleh organisasi dan perusahaan (Union, 2018). Aturan ini menetapkan prinsip-prinsip utama seperti legitimasi pengolahan data, hak akses individu, serta mekanisme sanksi untuk pelanggaran data (Schwartz & Solove, 2011).

Selain GDPR Uni Eropa juga memiliki *Directive on Security of Network and Information Systems* (NIS Directive) yang bertujuan untuk memperkuat ketahanan siber di sektor-sektor penting seperti energi, transportasi, dan perbankan (Commission, 2016). Dengan regulasi ini setiap negara anggota Uni Eropa diwajibkan untuk memiliki badan nasional yang bertanggung jawab atas keamanan siber dan mekanisme kerja sama antar negara dalam menghadapi ancaman siber (Carrapico & Barrinha, 2017). Uni Eropa juga meluncurkan *Digital Services Act* (DSA) dan *Digital Markets Act* (DMA) yang bertujuan untuk mengatur platform digital besar agar lebih transparan dalam pengelolaan data serta menjamin keadilan dalam persaingan digital (Commission, 2022). Regulasi ini memberlakukan hukuman yang tegas terhadap perusahaan teknologi yang tidak dapat memenuhi norma perlindungan data dan keterbukaan (Bradford, 2020).

Uni Eropa memiliki kerangka hukum siber yang lebih berkembang dan komprehensif. GDPR, NIS Directive dan regulasi digital lainnya menyediakan dasar hukum yang kokoh untuk mengatasi ancaman siber global. Pelaksanaan regulasi ini didukung oleh badan pengawas independen seperti *European Data Protection Board* (EDPB) yang menjamin kepatuhan terhadap peraturan yang telah ditentukan (Goddard, 2017). Tantangan terbesar dalam penerapan peraturan hukum siber di Uni Eropa adalah variasi pelaksanaan di setiap negara anggota serta kerumitan dalam penegakan hukum yang melintasi batas. Walaupun begitu metode Uni Eropa dalam pengaturan hukum siber bisa dijadikan acuan bagi Indonesia untuk merumuskan kebijakan yang lebih menyeluruh dan responsif terhadap perkembangan ancaman siber global.

Regulasi Hukum Siber di Amerika Serikat

Regulasi hukum siber di Amerika Serikat menerapkan pendekatan sektoral yang berarti bahwa pengaturan dilakukan sesuai dengan jenis industri atau sektor tertentu (Greenleaf, 2019). Berbeda dengan Uni Eropa yang memiliki regulasi umum seperti GDPR Amerika Serikat memiliki beragam undang-undang yang mengatur aspek hukum siber secara terpisah.

Di Amerika Serikat belum ada undang-undang federal yang secara keseluruhan mengatur perlindungan data dan privasi. Namun terdapat beberapa regulasi sektoral yang mengatur aspek ini di antaranya *Health Insurance Portability and Accountability Act* (HIPAA) yang mengatur perlindungan data kesehatan (Smith, 2020), *Gramm-Leach-Bliley Act* (GLBA) yang mengatur perlindungan data keuangan, *Children's Online Privacy Protection Act* (COPPA) yang mengatur perlindungan data anak-anak di bawah 13 tahun (Government, 2022), serta *California Consumer Privacy Act* (CCPA) yang merupakan regulasi perlindungan data

yang berlaku di negara bagian California dan sering dibandingkan dengan GDPR di Uni Eropa (Warren & Brandeis, 2018).

Beberapa undang-undang penting yang mengatur kejahatan siber di Amerika Serikat meliputi *Computer Fraud and Abuse Act* (CFAA) yang menjadikan akses ilegal ke sistem komputer sebagai kejahatan *Electronic Communications Privacy Act* (ECPA) yang melindungi komunikasi elektronik dari penyadapan yang tidak sah dan *Cybersecurity Information Sharing Act* (CISA) yang mendorong kolaborasi informasi tentang ancaman siber antara sektor publik dan swasta (Technology, 2021).

Peraturan di Amerika Serikat juga menekankan interaksi antara pemerintah dan sektor swasta dalam keamanan siber. Kerangka kerja keamanan siber dari *National Institute of Standards and Technology* (NIST) menjadi acuan keamanan siber yang diterapkan oleh perusahaan swasta dan instansi pemerintah untuk memperkuat ketahanan terhadap serangan siber (Greenleaf, 2019). Selain itu ada *Federal Information Security Modernization Act* (FISMA) mengatur perlindungan informasi untuk instansi pemerintah federal agar sistem informasi mereka aman dari serangan siber (Smith, 2020).

Dibandingkan dengan Uni Eropa yang menerapkan GDPR sebagai regulasi tunggal untuk mengatur privasi data secara menyeluruh pendekatan sektoral yang diambil oleh Amerika Serikat bisa menyebabkan fragmentasi dalam perlindungan data. Walaupun dapat disesuaikan dan fleksibel untuk kebutuhan sektor tertentu pendekatan ini juga memiliki kekurangan dalam hal keselarasan regulasi (Government, 2022). Indonesia bisa belajar dari kedua sistem ini untuk mengembangkan regulasi yang lebih responsif terhadap kemajuan teknologi dan ancaman siber global (Warren & Brandeis, 2018).

Perbandingan Regulasi Indonesia, Uni Eropa dan Amerika Serikat

Salah satu faktor mendasar dalam hukum siber adalah penjagaan data pribadi. Indonesia telah meratifikasi Undang-Undang No. 27 Tahun 2022 mengenai Perlindungan Data Pribadi (UU PDP) yang merupakan kemajuan dalam menetapkan landasan hukum untuk perlindungan data pribadi. Jika dibandingkan dengan peraturan di Uni Eropa dan Amerika Serikat, UU PDP masih memiliki beberapa kekurangan dalam pelaksanaan dan penegakan hukumnya. Uni Eropa memiliki *General Data Protection Regulation* (GDPR), yang merupakan salah satu regulasi perlindungan data paling ketat di seluruh dunia. GDPR menetapkan prinsip transparansi, hak akses bagi individu, serta mekanisme sanksi yang ketat terhadap pelanggaran. Tidak seperti Indonesia yang masih berada di fase awal penerapan UU PDP, GDPR sudah diterapkan sejak 2018 dan memiliki sistem pengawasan yang kokoh melalui *European Data Protection Board* (EDPB). Keunggulan GDPR terletak pada jangkauannya yang luas yang tidak hanya mengikat

perusahaan dalam Uni Eropa tetapi juga organisasi di luar Uni Eropa yang memproses data warga Uni Eropa. Amerika Serikat menerapkan pendekatan sektoral dalam perlindungan data pribadi yang menunjukkan bahwa regulasi yang berbeda diterapkan untuk sektor-sektor tertentu. Sebagai contoh adalah *Health Insurance Portability and Accountability Act* (HIPAA) untuk data kesehatan, *Gramm-Leach-Bliley Act* (GLBA) untuk data keuangan, serta *Children's Online Privacy Protection Act* (COPPA) untuk perlindungan data anak-anak. Negara bagian California telah mengesahkan *California Consumer Privacy Act* (CCPA) yang mirip dengan GDPR. Pendekatan sektoral ini seringkali menimbulkan fragmentasi dalam perlindungan data, berbeda dengan Uni Eropa yang memiliki regulasi yang konsisten. Untuk perbandingannya Indonesia masih harus meningkatkan mekanisme penegakan hukum yang lebih tegas agar UU PDP dapat dijalankan dengan efektif, selain itu harus ada penguatan lembaga pengawas perlindungan data agar lebih independen dan mampu menegakkan regulasi dengan lebih tegas.

Dalam menghadapi kejahatan siber, Indonesia menerapkan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). UU ini mengatur berbagai kejahatan siber, termasuk pencemaran nama baik, penyebaran informasi palsu, serta akses tanpa izin terhadap sistem elektronik. Tetapi UU ITE sering kali mendapatkan kritik karena dapat ditafsirkan secara beragam dan berisiko mengurangi kebebasan berekspresi. Beberapa ketentuan dalam UU ITE dinilai dapat disalahgunakan untuk menindak individu tanpa alasan yang tegas. Sedangkan Uni Eropa memiliki *Directive on Security of Network and Information Systems* (NIS Directive) yang bertujuan meningkatkan ketahanan siber dalam sektor-sektor penting seperti transportasi, energi dan perbankan. Uni Eropa juga mengatur platform digital lewat *Digital Services Act* (DSA) dan *Digital Markets Act* (DMA) yang bertujuan untuk menjamin keterbukaan dalam pengelolaan data serta menghindari praktik monopoli di ranah digital. Penegakan hukum siber di Uni Eropa lebih terstruktur karena adanya kolaborasi antara negara anggota serta lembaga pengawas independen yang memantau pelaksanaan regulasi. Di Amerika Serikat ada beberapa hukum yang mengatur kejahatan siber, seperti *Computer Fraud and Abuse Act* (CFAA) yang menjadikan akses ilegal ke sistem komputer sebagai tindak pidana serta *Electronic Communications Privacy Act* (ECPA) yang melindungi pesan elektronik dari penyadapan yang tidak sah. Sedangkan *Cybersecurity Information Sharing Act* (CISA) mendorong kolaborasi antara pemerintah dan sektor swasta dalam pertukaran informasi mengenai ancaman siber. Regulasi ini menunjukkan pendekatan yang lebih luwes dari Amerika Serikat dalam menghadapi kejahatan siber dengan menekankan kolaborasi dengan sektor swasta. Jika dilihat dari perspektif yang lain pendekatan Uni Eropa lebih menyeluruh dalam mengatasi kejahatan siber dengan regulasi yang terpadu dan sistem pengawasan yang ketat. Amerika Serikat

menggunakan kombinasi regulasi dan kolaborasi dengan sektor swasta sedangkan Indonesia masih menghadapi tantangan penafsiran ganda dalam UU ITE yang perlu diperbaiki agar lebih efisien dan tidak disalahgunakan.

Dalam konteks penyelarasan kebijakan Uni Eropa memiliki sistem yang lebih terorganisir karena regulasi seperti GDPR dan NIS Directive diterapkan secara konsisten di seluruh negara anggota. Walaupun terdapat tantangan dalam perbedaan implementasi di masing-masing negara anggota, pendekatan Uni Eropa tetap lebih terkoordinasi dibandingkan dengan Indonesia dan Amerika Serikat. Indonesia masih menghadapi kesulitan dalam menyelaraskan regulasi hukum siber dengan standar global. Salah satu permasalahan utama adalah ketidakcocokan antara UU PDP dan UU ITE serta belum adanya persetujuan terhadap Konvensi Budapest mengenai Kejahatan Siber. Konvensi Budapest adalah standar global untuk menangani kejahatan siber, dan sampai saat ini Indonesia belum bergabung dalam perjanjian itu, sehingga kolaborasi internasional dalam penegakan hukum siber masih terbatas. Amerika Serikat juga mengalami kesulitan dalam menyamakan regulasi akibat pendekatan sektoralnya. Dengan adanya berbagai undang-undang yang mengatur perlindungan data dan kejahatan siber secara terpisah, konsistensi dalam penerapan regulasi sering kali menjadi masalah. Namun keluwesan peraturan di Amerika Serikat memungkinkan penyesuaian terhadap kemajuan teknologi yang pesat. Jika diperbandingkan Uni Eropa memiliki peraturan yang paling terstandarisasi dan ketat, sedangkan Amerika Serikat memberikan fleksibilitas melalui pendekatan sektoralnya. Di lain sisi Indonesia masih perlu meningkatkan regulasi yang lebih sesuai dengan standar internasional untuk lebih efektif menghadapi ancaman siber global

5. KESIMPULAN DAN SARAN

Regulasi hukum siber di Indonesia masih mendapatkan berbagai tantangan dalam menghadapi ancaman internasional. Meski sudah ada UU PDP, pelaksanaan dan penegakan hukumnya masih perlu ditingkatkan. Tidak seperti Uni Eropa yang telah menerapkan GDPR dengan sistem perlindungan data yang ketat, peraturan di Indonesia masih belum sepenuhnya sejalan dengan standar internasional. Dalam menangani kejahatan siber, koordinasi antar instansi penegak hukum di Indonesia masih kurang baik, sedangkan Amerika Serikat dengan pendekatannya yang sektoral dapat beradaptasi lebih cepat terhadap ancaman yang ada.

Penelitian ini menyarankan peningkatan keselarasan peraturan hukum siber di Indonesia dengan standar internasional agar dapat lebih tanggap terhadap ancaman global. Pengembangan kapasitas institusi dan kolaborasi antar lembaga hukum siber harus diutamakan dalam penerapan kebijakan. Kerjasama internasional melalui kesepakatan bilateral dan

keterlibatan dalam forum global juga penting untuk memperkokoh posisi Indonesia di arena internasional. Langkah-langkah ini diharapkan dapat memperkuat kesiapan peraturan hukum siber di Indonesia. Penelitian ini juga memberikan kesempatan untuk penelitian tambahan mengenai efektivitas kebijakan yang diimplementasikan dan pengaruhnya terhadap keamanan siber nasional.

DAFTAR REFERENSI

Bradford, A. (2020). *The Brussels effect: How the European Union rules the world*. Oxford University Press. https://doi.org/10.1093/oso/9780190088583.001.0001

Carrapico, H., & Barrinha, A. (2017). The European Union's cybersecurity strategy: A critical analysis. *European Security, 26*(2), 130–151.

European Commission. (2016). *Directive on security of network and information systems (NIS Directive)*. https://ec.europa.eu/digital-strategy

European Commission. (2022). *Digital services act and digital markets act*. https://ec.europa.eu/digital-strategy

Firmansyah, A. (2020a). Regulasi perlindungan data pribadi di Indonesia: Tantangan dan prospek. *Jurnal Hukum dan Teknologi, 12*(2), 45–60.

Firmansyah, A. (2020b). Regulasi perlindungan data pribadi di Indonesia: Tantangan dan prospek. *Jurnal Hukum dan Teknologi, 12*(2), 45–60.

Goddard, M. (2017). The EU general data protection regulation (GDPR): European regulation that has a global impact. *International Journal of Law and Information Technology, 25*(3), 171–197.

Government of California. (2022). *California consumer privacy act (CCPA)*. https://www.oag.ca.gov/privacy/ccpa

Greenleaf, G. (2019). *Global data privacy laws: The U.S. vs the EU*. Cambridge University Press.

Kusuma, H., & Wibisono, R. (2022). Penegakan hukum kejahatan siber di Indonesia: Tantangan dan solusi. *Jurnal Hukum Siber, 7*(1), 23–40.

Marzuki, P. M. (2017). *Penelitian hukum*. Kencana.

NIST. (2021). *Cybersecurity framework*. National Institute of Standards and Technology.

Nugroho, A. (2023). *Regulasi perlindungan data di Amerika Serikat: Tinjauan atas CCPA dan dampaknya*. Pustaka Digital.

Pratama, R., & Suhendar, T. (2022). *Dinamika penerapan UU ITE dalam masyarakat Indonesia*. Gadjah Mada University Press.

Putri, L. (2023). *Perlindungan data pribadi di Indonesia: Implementasi dan tantangan*. CV Media Hukum.

Schwartz, P. M., & Solove, D. J. (2011). The PII problem: Privacy and a new concept of personally identifiable information. *New York University Law Review, 86*(6), 1814–1894.

Setyowati, R. (2021). Evaluasi regulasi hukum siber di Indonesia: Perspektif global. *Jurnal Hukum Teknologi*, *10*(4), 50–72.

Siregar, M., & Hidayat, T. (2023). *Kejahatan siber dan upaya penegakan hukum di Indonesia*. Penerbit Hukum Nasional.

Smith, J. (2020). *Cybersecurity law and policy*. Oxford University Press.

Solms, R. von, & Niekerk, J. van. (2013). From information security to cyber security. *Computers & Security, 38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

Union, E. (2018). *General data protection regulation (GDPR)*. European Union.

Warren, S., & Brandeis, L. (2018). The right to privacy. *Harvard Law Review*.

Wijaya, D. (2021). *Cybersecurity and legal challenges in Indonesia: Towards international harmonization*. Cyber Law Journal.