INNOVATIVE: Journal Of Social Science Research
Volume 4 Nomor 5 Tahun 2024 Page 4340-4357
E-ISSN 2807-4238 and P-ISSN 2807-4246
Website: https://j-innovative.org/index.php/Innovative

Pemanfaatan Skema *Common Criteria* Indonesia Terhadap Produk TIK Berdasarkan Peraturan BSSN Nomor 15 Tahun 2019 dengan Perbandingan Implementing Regulation (EU) 2024/482

Siti Nahrisya Nur Gayatri[1✉], Muhamad Amirulloh[2], Mustofa Haffas[3]
Universitas Padjadjaran
Email: siti20041@mail.unpad.ac.id[1✉]

Abstrak

Indonesia dan Uni Eropa memiliki perbedaan dalam melindungi keamanan produk TIK melalui sertifikat *common criteria* yang dilandasi pada ISO/IEC 15408 dan ISO/IEC 18045. Perbedaan tersebut dilihat dari prosedur sertifikasi, tingkat jaminan keamanan, dan pemeliharaan jaminan keamanan. Tujuan penelitian ini untuk menganalisis pelindungan hukum dan bentuk pelindungan hukum yang efektif di Indonesia terhadap produk TIK dalam pemanfaatan sertifikat *common criteria*. Penelitian ini menggunakan metode pendekatan yuridis normatif, yaitu yuridis komparatif antara Indonesia dan Uni Eropa. Hasil penelitian ini diketahui bahwa pelindungan hukum Indonesia lebih rendah daripada Uni Eropa melihat keamanan produk TIK diatur secara komprehensif serta bentuk pelindungan hukum yang tepat dan dapat diadopsi dari Uni Eropa dengan memperhatikan empat unsur pelindungan hukum.

Kata Kunci: *Common Criteria*, *Kemanan Produk TIK, Jaminan Keamanan*

Abstract

Indonesia and the European Union have differences in protecting the security of ICT products through common criteria certificates based on ISO/IEC 15408 and ISO/IEC 18045. The differences are seen from the certification procedure, the level of security assurance, and the maintenance of security assurance. The purpose of this study is to analyze the legal protection and effective form of legal protection in Indonesia against ICT products in the utilization of common criteria certificates. This research uses normative juridical approach method, namely comparative juridical between Indonesia and the European Union. The results of this study found that Indonesia's legal protection is lower than the European Union seeing the security of ICT products is comprehensively regulated as well as the appropriate form of legal protection and can be adopted from the European Union by taking into account the four elements of legal protection.
Keywords: *Common Criteria, ICT Product Security, Security Assurance*

PENDAHULUAN

Pesatnya perkembangan teknologi informasi dan komunikasi berhubungan erat dengan disrupsi teknologi yang mengakibatkan adanya perubahan keberlangsungan masyarakat secara signifikan. Disrupsi digital membuat keamanan siber menjadi urgensi untuk dilindungi. Keamanan siber merupakan kumpulan teknologi, proses, dan praktik untuk melindungi dunia siber terhadap organisasi dan aset pengguna dari ancaman dan serangan siber (Putranto, 2023). Keamanan siber tidak hanya mengamankan sistem elektronik, tetapi juga komponen sistem elektronik berupa *hardware* dan *software*.

Berdasarkan Pasal 23 Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik ("PP PSTE") mewajibkan Penyelenggara Sistem Elektronik (PSE) untuk mengamankan komponen sistem elektronik yang melingkupi *hardware* dan *software*. Selanjutnya, Peraturan BSSN No. 15 Tahun 2019 tentang Penyelenggaraan Skema *Common Criteria* Indonesia ("PBSSN 15/2019") mengatur lebih mendalam terkait pelaksanaan pengamanan produk TIK.

Berdasarkan PBSSN 15/2019, skema ini didasari pada *Common Criteria* (CC) yang berlandaskan pada standar evaluasi keamanan teknologi informasi yang disesuaikan dengan ISO/IEC 15408 dan ISO/IEC 18045 yang merupakan gambaran dan aturan mengenai pedoman sertifikasi keamanan produk teknologi informasi untuk meningkatkan daya saing Indonesia dan

membangun kepercayaan konsumen yang diberikan atas dasar jaminan keamanan. Dalam mensertifikasi SCCI terdapat tiga tahap, yakni permohonan CC Indonesia, pelaksanaan evaluasi TOE atau PP, dan penetapan keputusan sertifikasi sebagaimana dimaksud pada Pasal 3 PBSSN 15/2019. Selanjutnya, untuk melakukan permohonan sertifikasi CC, terdiri dari permohonan sertifikasi TOE (*Target of Evaluation*) dan PP (*Protection Profiles*) yang nantinya akan diverifikasi oleh Lembaga Sertifikasi Produk CC Indonesia (LSPro) dan laboratorium pengujian untuk menempatkan kelas jaminan. Setelah itu, akan dilakukan penetapan keputusan sertifikasi. Sementara itu, pemeliharaan jaminan keamanan dilakukan apabila adanya perubahan atau penambahan fitur keamanan.

Walaupun telah diatur, tetapi keamanan siber di Indonesia masih terbelakang apabila dibandingkan dengan negara-negara Uni Eropa (Laporan National Cyber Security Index, 2023). Terlebih lagi, banyaknya kasus kejahatan siber di Indonesia yang salah satunya adalah penyerangan siber terhadap Pusat Data Nasional (PDN) Sementara yang diserang oleh *ransomware* jenis baru, yaitu LockBit 3.0 Brain Chiper (Ernis, 2024). Serangan ini berdampak pada ratusan instansi pemerintah pusat dan daerah bahkan data masyarakat sudah tidak dapat lagi dipulihkan (Bhayangkara, 2024). Berdasarkan kasus tersebut diketahui bahwa penyebab penyerangan siber dilakukan oleh *ransomware*, yaitu berupa perangkat lunak berbahaya atau *malicious software* (*malware*) yang cara kerjanya adalah menyerang perangkat korban dengan mengenkripsi data atau dokumen di dalamnya. Selain itu, modus kejahatan ini meminta uang tebusan kepada korban untuk bisa membuka data yang telah terenkripsi tersebut (Hardiansyah, 2024). Seharusnya, melalui PBSSN 15/2019 dapat meminimalisasi serangan siber jenis tersebut terhadap Produk TIK.

Dalam hal ini, sebaliknya telah diatur secara komprehensif oleh Uni Eropa melalui Regulation (EU) 2019/881 atau EU Cybersecurity Act dan peraturan turunannya berupa Commission Implementing Regulation (EU) 2024/482 atau Implementing Regulation (EU) 2024/482. EU Cybersecurity Act mengatur skema dan sertifikasi keamanan siber berdasarkan jenis layanan TIK, yaitu *ICT Product* (*hardware*, *software*, dan *firmware*), *ICT Service* (*cloud computing* dan *big data*), dan *ICT Process* (melindungi *ICT Product* dan *Service*) sebagaimana

diatur pada Article 2 EU Cybersecurity Act. Untuk melindunginya, diperlukan penerapan tingkat jaminan (*basic, high,* dan *substantial)* diperlukan untuk melindungi layanan TIK dari serangan siber sesuai dengan risiko yang dihadapi (Dutch NCCA, 2024). EU Cybersecurity Act mengeluarkan beberapa skema sertifikasi, yaitu EUCC, EUCS, EU5G, dan akan dikembangkan lebih lanjut.

Dalam penelitian ini, membahas skema EUCC untuk melindungi *ICT Product* melalui Implementing Regulation (EU) 2024/482. Berdasarkan peraturan ini juga berbasis pada ISO/IEC 15408 dan ISO/IEC 18045. Namun, mengkhususkan lagi ISO/IEC 15408 digunakan sebagai penggunaan standar CC, sementara ISO/IEC 18045 digunakan untuk penggunaan metodologi evaluasi umum sebagaimana dimaksud pada *Article* 3 Implementing Regulation (EU) 2024/482. Melalui skema ini, terdapat dua pilihan dalam mensertifikasi suatu *ICT Product* terhadap *Security Target* (ST) yang ditentukan pada pemohon sertifikat atau menggabungkan sertifikat PP sebagai bagian dari *ICT Process* yang didalamnya sudah terdapat kategori *ICT Product*. Selain itu, diwajibkan untuk mensertifikasi PP sebelum mensertifikasi *ICT Product*. Dalam skema ini, terdapat dua aspek jaminan keamanan, yaitu *Evaluation Assurance Level* (EAL) yang terkait dengan standar ISO/IEC 15408, dan *Vulnerability Analysis* (AVA_VAN Level) berdasarkan Article 52 EU Cybersecurity Act (*high* dan *substantial*). EAL mengukur tingkat evaluasi dari 1-7, sementara AVA_VAN Level menentukan skala 1-5 untuk menentukan tingkat jaminan keamanan. Perbedaannya, EAL menilai tingkat kepercayaan evaluasi keamanan pada ICT Product, sedangkan AVA_VAN Level menentukan tingkat analisis kerentanan terhadap evaluasi keamanan untuk menentukan tingkat ketahanan terhadap kelemahan pada TOE.

Beberapa persyaratan untuk mensertifikasi PP adalah menerapkan standar CC dan metodologi evaluasi umum, AVA_VAN Level, serta menyiapkan dokumen teknis dan dokumen mutakhir. Setelah itu, beberapa persyaratan untuk mensertifikasi *ICT Product* adalah memenuhi standar CC dan metodologi evaluasi umum, EAL, AVA_VAN Level, dokumen mutakhir, dan sertifikat PP. Dalam memeliharanya, pemegang sertifikat EUCC harus menerapkan prosedur manajemen kerentanan dengan analisis dampak dan laporan perubahan yang disesuaikan dengan standar EN ISO/IEC 30111.

Identifikasi masalah dalam penelitian ini adalah pertama, bagaimana pelindungan hukum produk TIK terhadap pemanfaatan CC berdasarkan PBSSN 15/2019 dengan perbandingannya Implementing Regulation (EU) 2024/482? Kedua, bagaimana bentuk pelindungan hukum yang tepat dan dapat diterapkan dari Uni Eropa? Sementara itu, tujuan penelitian adalah menganalisis perlindungan hukum dan bentuk pelindungan hukum yang efektif terhadap produk TIK dalam pemanfaatan sertifikat CC Indonesia.

METODE PENELITIAN

Dalam penelitian ini, menggunakan metode pendekatan berupa yuridis normatif, yaitu dengan meneliti bahan kepustakaan atau data sekunder sebagai bahan penelitian utama, pada khususnya menggunakan yuridis komparatif (perbandingan hukum) antara Indonesia dan Uni Eropa. Subjek dari penelitian ini adalah PSE sebagai pengguna sertifikat SCCI, sementara objek penelitian ini adalah perbandingan hukum mengenai SCCI antara Indonesia dan Uni Eropa. Teknik untuk mengumpulkan data menggunakan studi kepustakaan dengan mengumpulkan, menelusuri, dan menelaah bahan-bahan hukum. Selanjutnya, metode analisis yang digunakan bersifat kualitatif dengan mendeskripsikan temuan-temuan hukum serta menggunakan metode deduktif berupa menarik kesimpulan dari suatu permasalahan yang bersifat umum terhadap permasalahan konkret yang dihadapi.

HASIL DAN PEMBAHASAN

A. Pelindungan Hukum Terhadap Produk TIK dalam Pemanfaatan Sertifikat Common Criteria bagi Masyarakat Indonesia berdasarkan PBSSN 15/2019 dan perbandingannya dengan Implementing Regulation (EU) 2024/482

Menurut Satjipto Raharjo, pelindungan hukum adalah upaya untuk melindungi kepentingan seseorang melalui cara mengalokasikan suatu kekuasaan kepadanya, salah satu sifat serta tujuan dari hukum adalah untuk memberikan perlindungan kepada masyarakat (Satjipto Raharjo, 1983). Pelindungan hukum tersebut diwujudkan dengan adanya kepastian hukum sehingga masyarakat dapat menikmati seluruh hak-hak yang diberikan oleh hukum

sebagai bentuk perlindungan hukum kepada masyarakat (Satjipto Raharjo, 2000). Dalam mewujudkan perlindungan hukum, terdapat empat unsur yang perlu dipenuhi, yaitu adanya perlindungan atau pengayoman dari pemerintah kepada warganya; jaminan kepastian hukum; berkaitan dengan hak-hak warga negaranya; dan adanya sanksi hukum bagi pihak yang melanggarnya (Hetty Hasanah, 2004). Dalam hal ini, keamanan suatu produk TIK melalui sertifikat CC sangatlah penting untuk memberikan jaminan keamanan terhadap masyarakat dalam menggunakan suatu produk TIK.

Dalam menggunakan perangkat keras yang terhubung dalam sistem elektroniknya, PSE wajib untuk memenuhi aspek keamanan, interkonektivitas, dan kompatibilitas dengan sistem yang digunakan; memiliki layanan dukungan teknis, pemeliharaan, dan/atau purnajual dari penjual atau penyedia; dan memiliki jaminan keberlanjutan layanan sebagaimana dimaksud pada Pasal 7 ayat (1) PP PSTE. Sementara itu, untuk memenuhi persyaratan tersebut wajib dilakukan sertifikasi atas perangkat keras atau bukti-bukti sejenisnya yang telah diatur dalam Pasal 7 ayat (2) PP PSTE. Selain itu, berdasarkan Pasal 8 PP PSTE, PSE harus menggunakan perangkat lunak yang keamanan dan keandalan operasinya terjamin dan kepastian terhadap keberlanjutan layanan. Dalam mengamankan penyelenggaraan sistem elektronik, PSE wajib untuk mengamankan komponen sistem elektronik, komponen sistem elektronik yang dimaksud termasuk pula perangkat keras dan lunak sebagaimana dimaksud pada Pasal 23 jo. Penjelasan Pasal 23 PP PSTE.

Selanjutnya, untuk mengamankan perangkat keras dan perangkat lunak tersebut diatur lebih mendalam pada PBSSN 15/2019, tetapi tidak tertulis secara langsung hubungan antara PP PSTE dengan PBSSN 15/2019 dan perlu diketahui bahwa PBSSN 15/2019 merupakan satu-satunya peraturan yang mengatur akan hal ini. Dalam PBSSN 15/2019 tidak mengenal PSE sebagai pihak yang berkepentingan, tetapi mengenal dengan Sponsor dan Developer sebagai pihak yang mensertifikasi produk TIK mereka. Berdasarkan Pasal 1 angka 13 PBSSN 15/2019, Sponsor adalah perusahaan atau perseorangan yang mensponsori suatu TOE atau PP yang akan disertifikasi. Sementara itu, Developer adalah perusahaan atau perseorangan yang mengembangkan suatu TOE atau PP sebagaimana dimaksud pada Pasal 1 angka 14 PBSSN

15/2019. Berdasarkan penjelasan ini, hubungan antara Sponsor, Developer, dan PSE memiliki peran dan fokus yang berbeda, tetapi masih saling berhubungan. Hubungan tersebut dapat dilihat ketika menerapkan standar keamanan dan kepatuhan berdasarkan SCCI terhadap produk TIK, terdapat dua kemungkinan, yaitu PSE bertindak sebagai Sponsor dan/atau Developer untuk mengembangkan dan mengajukan sertifikasi untuk sistem elektroniknya. Kedua, PSE dapat bekerja sama dengan pihak ketiga yang berperan sebagai Sponsor dan/atau Developer dalam proses sertifikasi SCCI.

Dalam memohonkan sertifikasi CC Indonesia, Sponsor atau Developer melampirkan permohonan sertifikasi TOE dan PP. Untuk permohonan sertifikasi TOE, beberapa dokumen yang perlu disiapkan adalah formulir aplikasi permohonan sertifikasi TOE, ST, *Evaluation Project Proposal*, surat pernyataan penilaian awal ST dan bukti evaluasi, dan TOE. Sementara itu, dalam mengajukan permohonan sertifikasi PP, dokumen yang dibutuhkan adalah formulir aplikasi permohonan sertifikasi PP, *Evaluation Project Proposal*, dan PP. Setelah itu, permohonan tersebut akan diverifikasi oleh LSPro terkait kelengkapan persyaratan dan substansi dokumen. Selanjutnya, akan dilakukan evaluasi terhadap TOE dan PP tersebut oleh Laboratorium Pengujian untuk mengevaluasi audit dokumen ST dan bukti evaluasi TOE, pengujian fungsionalitas, dan pengujian penilaian kerentanan TOE. Pelaksanaan evaluasi ini juga diawasi oleh LSPro. Setelah itu, LSPro akan menetapkan keputusan sertifikasi terkait lulus atau tidaknya sertifikasi terhadap produk TIK tersebut. Untuk memelihara keamanan produk TIK tersebut, perlu untuk melakukan pemeliharaan jaminan keamanan yang sifatnya tidak wajib oleh Sponsor atau Developer apabila terdapat perubahan atau penambahan fitur keamanan terhadap TOE untuk meningkatkan jaminan keamanan.

Sebagai perbandingan hukum, Uni Eropa juga mengatur hal yang sama melalui Implementing Regulation (EU) 2024/482 sebagai peraturan turunan dari EU Cybersecurity Act. Berdasarkan ketentuan tersebut, pihak yang ingin mensertifikasi adalah seluruh produsen dan penyedia yang ingin menilai kualitas produk TIK-nya melalui sertifikasi pihak ketiga dengan mengajukan permohonan sertifikasi EUCC. Tujuan Uni Eropa dalam mengimplementasikan EUCC *Scheme* dan mengaturnya adalah untuk memfasilitasi pengakuan bersama terhadap

sertifikasi di seluruh negara anggota sehingga hal ini sebagai bentuk harmonisasi sertifikasi pada *ICT Product*. Dengan harmonisasi, akan memungkinkan suatu *ICT Product* diperdagangkan lebih mudah di antara negara-negara anggota sehingga dapat menyederhanakan proses sertifikasi bagi produsen dan menumbuhkan kepercayaan serta kerja sama di antara negara-negara anggota (ENISA, 2024).

Ruang lingkup Implementing Regulation (EU) 2024/482 berdasarkan *Article* 1 adalah keberlakuan EUCC *Scheme* kepada semua *ICT Product* termasuk dokumentasinya serta semua PP yang diajukan untuk sertifikasi sebagai bagian dari *ICT Process* yang mengarah pada sertifikasi *ICT Product*. Standar yang digunakan sama dengan SCCI, yakni CC berlandaskan ISO/IEC 15408 dan Metodologi Evaluasi Umum yang berlandaskan ISO/IEC 18045 sebagaimana diatur dalam Article 3 Implementing Regulation (EU) 2024/482. Terdapat dua metode untuk mensertifikasi *ICT Product*, antara lain, pertama, dalam hal mensertifikasi suatu *ICT Product* harus melakukan suatu tindakan untuk ST, yaitu ditentukan oleh pemohon atau menggabungkan PP bersertifikat sebagai bagian dari *ICT Process* ketika *ICT Product* termasuk dalam kategorinya yang melingkupi pula dalam PP tersebut. Kedua, PP wajib disertifikasi untuk dapat mensertifikasi *ICT Product*.

Dalam skema EUCC, mengenal dua hal terkait jaminan keamanan, yakni EAL yang melekat pada standar ISO/IEC 15408 atau CC dengan skala 1 hingga 7 dan AVA_VAN Level yang melekat pada pengaturan Article 52 EU Cybersecurity Act dengan dua tingkat jaminan serta memiliki skala 1 hingga 5. Keduanya memiliki perbedaan tujuan, pada EAL bertujuan untuk menilai tingkat kepercayaan evaluasi keamanan terhadap *ICT Product* yang menentukan kedalaman evaluasi keamanan yang telah dilakukan dan keandalan berdasarkan hasil evaluasi dan tingkat kepercayaan tersebut. Di lain sisi, pada AVA_VAN Level merupakan suatu tingkat analisis kerentanan jaminan untuk menunjukkan tingkat kegiatan evaluasi keamanan siber untuk menentukan tingkat ketahanan terhadap kelemahan pada TOE. Untuk mensertifikasi EUCC wajib untuk diterbitkan secara bersamaan terkait tingkat jaminan berdasarkan AVA_VAN Level, yaitu pada tingkat *substantial* dengan AVA_VAN Level 1 atau 2 dan *high* dengan AVA_VAN Level 3, 4, atau 5 sebagaimana diatur dalam Article 15 Para 1 Implementing Regulation (EU)

2024/482.

Untuk mensertifikasi EUCC, diwajibkan untuk mensertifikasi PP terlebih dahulu dengan adanya kewajiban untuk mengevaluasi beberapa persyaratan, yaitu mengimplementasikan standar dalam CC dan metodologi evaluasi umum, tingkat jaminan berdasarkan AVA_VAN Level dan persyaratan keamanan yang dimaksud pada Article 51 EU Cybersecurity Act, serta dokumen teknis dan dokumen mutakhir. Setelah memperoleh sertifikat PP, perlu untuk mensertifikasi *ICT Product* dengan beberapa persyaratan minimal, yaitu memenuhi standar CC dan metodologi evaluasi umum, EAL sebagai jaminan keamanan untuk menilai kerentanan dan pengujian fungsional independen, tingkat jaminan yang berdasarkan AVA_VAN Level dan persyaratan keamanan yang dimaksud pada Article 51 EU Cybersecurity Act, dokumen mutakhir, serta sertifikat PP. Bentuk pemeliharaan sertifikat EUCC, pemegang sertifikat diwajibkan untuk menerapkan prosedur manajemen kerentanan untuk memastikan apakah prosedur dari standar berdasarkan skema EUCC ini berjalan. Apabila terjadi potensi kerentanan siber, pemegang sertifikat diwajibkan untuk menganalisis dampak kerentanan yang nantinya akan ditindaklanjuti oleh pihak berwenang, manajemen kerentanan ini disesuaikan dengan prosedur berdasarkan EN ISO/IEC 30111.

Berdasarkan tinjauan hukum terkait mekanisme dan perlindungan produk TIK yang dilandasi oleh ISO/IEC 15408 dan ISO/IEC 18045 antara Indonesia dan Uni Eropa memiliki beberapa perbedaan. Walaupun telah menggunakan standar yang sama dan juga tidak diwajibkan untuk menggunakannya, Uni Eropa mengaturnya lebih komprehensif untuk melindungi suatu produk TIK dengan mengatur mekanisme sertifikasi yang tidak hanya untuk *ICT Product*, tetapi juga untuk *ICT Process*. Selain itu, menambahkan tingkat jaminan berupa AVA_VAN Level yang nantinya akan menentukan produk TIK tersebut apakah termasuk kategori *substantial* atau *high* sehingga pemegang sertifikat akan mengetahui potensi kerentanan sibernya. Begitu pula dengan memelihara sertifikatnya dengan mewajibkan pemegang sertifikat untuk melakukannya sehingga nantinya akan diketahui potensi kerentanan siber yang dihadapi. Di lain sisi, Indonesia dalam mengatur hal ini masih terdapat beberapa kekurangan, yaitu tidak mengatur secara mendalam tujuan permohonan sertifikat PP dan TOE.

Selain itu, dalam proses evaluasi hanya mengenal terkait EAL, tetapi hal ini tidak diatur secara mendalam apa yang dimaksud dengan EAL dan bagaimana klasifikasinya serta hanya menguji suatu produk dengan EAL 3 (Arti, 2023). Tidak wajibnya melakukan pemeliharaan serta konsep yang berbeda untuk memelihara sertifikat SCCI juga menjadi poin kelemahan pada pengaturan ini. Terlebih lagi, tidak meluasnya pengaturan SCCI sehingga banyak perusahaan yang tidak mengetahui standardisasi dan sertifikat SCCI.

Oleh karena itu, masyarakat Indonesia sebagai konsumen dalam penggunaan produk TIK masih belum memperoleh perlindungan hukum terhadap produknya berupa jaminan keamanan. Apabila dibandingkan dengan EUCC di Uni Eropa, walaupun EUCC belum berlaku secara efektif, tetapi para pihak yang berkepentingan termasuk para pelaku usaha atau produsen produk TIK telah mempersiapkannya secara lebih komprehensif dengan menyesuaikan CC yang lama dengan patuh kepada skema EUCC. Maka dari itu, selain produsen dapat berinovasi sebelum mengeluarkan produk tersebut dengan mengintegrasikan fitur keamanan pada tahap pengembangan produk TIK, juga memberikan jaminan keamanan kepada masyarakat dalam menggunakan produknya.

B. Bentuk Pelindungan Hukum yang Tepat Terhadap Produk TIK Bagi Masyarakat Indonesia dan Dapat Diterapkan dari Uni Eropa

Terdapat empat unsur yang harus dipenuhi dalam mewujudkan pelindungan hukum, yakni:

1. Adanya Perlindungan atau Pengayoman dari Pemerintah Kepada Warganya

Melalui PBSSN 15/2019, Pemerintah telah mengatur mekanisme dan prosedur dalam mensertifikasi produk TIK berdasarkan ISO/IEC 15408 dan ISO/IEC 18045, tetapi dalam implementasinya masih belum dijalankan dengan baik. Hal ini diketahui bahwa masih banyak perusahaan dan masyarakat yang belum mengetahui peraturan ini sehingga belum memberikan jaminan keamanan terhadap produk TIK. Terlebih lagi, sumber daya manusia dan teknologi yang digunakan dalam mensertifikasi ini masih rendah dan biaya yang dikeluarkan relatif mahal (Ratih Mumpuni Arti (et.al), 2023).

Namun, EU Cybersecurity Act dan Implementing Regulation (EU) 2024/482 sebaliknya

diatur lebih komprehensif dan pengayoman yang lebih maksimal dari pemerintahnya. Hal ini diketahui bahwa prosedur dalam memperoleh sertifikat yang lebih komprehensif, tujuan dari sertifikasi *ICT Product* dan *ICT Process* yang lebih jelas melalui CC dan terstruktur, perolehan jaminan keamanan terhadap produk TIK lebih tinggi dengan memiliki dua jaminan keamanan (EAL dan AVA_VAN Level), serta kewajiban untuk pemeliharaan jaminan keamanan tersebut.

Maka dari itu, Komisi Uni Eropa dibantu dengan pihak-pihak yang berkepentingan, serta para ahli telah memberikan perlindungan secara lebih mendasar dan komprehensif serta memberikan pengayoman kepada masyarakat dan pelaku usaha walaupun peraturan ini belum berlaku secara efektif. Sementara, di Indonesia, pemerintah belum memberikan pengayoman secara lebih mendalam kepada pelaku usaha dan masyarakat terhadap pemberlakuan PBSSN 15/2019.

2. Jaminan Kepastian Hukum

Menurut Sudikno Mertokusumo, kepastian hukum adalah perlindungan yustisiabel terhadap tindakan sewenang-wenang, yang berarti bahwa seseorang akan dapat memperoleh sesuatu yang diharapkan dalam keadaan tertentu (Margono, 2022). Dalam hal ini, PBSSN 15/2019 dan Implementing Regulation (EU) 2024/482 telah mengatur *common criteria* sebagai salah satu standar untuk mengamankan suatu produk TIK.

Akan tetapi, dalam pelaksanaannya di Indonesia, hanya sedikit produk yang telah disertifikasi. Maka dari itu, tidak sesuai dengan tujuan awal atau harapan awal dari terbentuknya PBSSN 15/2019 yang disebabkan oleh faktor-faktor yang telah disebutkan sebelumnya. PBSSN 15/2019 terbentuk karena Indonesia telah menandatangani Common Criteria Recognition Agreement (CCRA), Indonesia dalam hal ini sebagai peserta pengguna sertifikat sehingga wajib untuk membentuk suatu peraturan terhadap CC di Indonesia. Hal ini telah menjadi langkah awal yang baik, tetapi perlu diperhatikan implementasi dalam menjalankan peraturan ini sehingga dapat mencapai tujuan dan harapan awal. Selain itu, melalui PBSSN 15/2019 lebih menitikberatkan tugas dan wewenang pihak-pihak di dalamnya, daripada prosedur dan teknis pemberlakuan sertifikat CC Indonesia sehingga ketentuan teknis sertifikasi tersebut tidak mengatur secara komprehensif.

Di sisi lain, Uni Eropa melalui Implementing Regulation (EU) 2024/482 terbentuk karena merupakan peraturan turunan dari EU Cybersecurity Act. Undang-Undang tersebut merupakan langkah Uni Eropa untuk mengharmonisasikan seluruh birokrasi melalui sertifikasi keamanan siber di Uni Eropa sehingga birokrasi lebih mudah dan biaya pun lebih murah. Pembuatan undang-undang ini pun melibatkan banyak pihak yang berkepentingan, seperti ENISA, para pemimpin negara, dan para ahli di bidang siber, hingga masyarakat umum. Oleh sebab itu, tujuan dari peraturan ini lebih jelas, objektif, dan terstruktur. Sementara itu, Implementing Regulation (EU) 2024/482 mengatur secara seimbang antara para pihak di dalamnya dan ketentuan teknis sehingga memberikan kepastian hukum yang lebih tinggi kepada masyarakatnya.

3. Berkaitan dengan Hak-Hak Warga Negaranya

Dengan memberikan kepastian hukum kepada masyarakatnya, Uni Eropa melalui Implementing Regulation (EU) 2024/482 sebagaimana telah dijelaskan sebelumnya, tentunya akan memberikan perlindungan terhadap hak-hak masyarakat Uni Eropa dalam keamanan produk TIK. Di sisi lain, PBSSN 15/2019 belum memberikan kepastian hukum terhadap karena faktor-faktor yang telah dijelaskan sebelumnya sehingga masyarakat Indonesia sebagai konsumen produk TIK tersebut belum memperoleh jaminan keamanan sebagai hak masyarakat.

4. Sanksi Hukum Bagi Pihak yang Melanggarnya

Dalam hal ini, tidak ada sanksi administratif apa pun berdasarkan PBSSN 15/2019, hanya saja dalam peraturan tersebut terdapat pengaturan terkait pencabutan sertifikat CC Indonesia apabila adanya penyalahgunaan sertifikat oleh Sponsor atau Developer; penyalahgunaan nama dan logo BSSN, LSPro, SCCI, dan/atau CCRA oleh Sponsor atau Developer; atau adanya konflik kepentingan yang menimbulkan keberpihakan dalam proses sertifikasi sebagaimana dimaksud pada Pasal 18 PBSSN 15/2019. Apabila ditinjau lebih awal, Pasal 23 PP PSTE mewajibkan PSE untuk mengamankan komponen sistem elektroniknya yang termasuk pula perangkat keras dan lunak sebagai produk TIK, apabila tidak mematuhi ketentuan tersebut akan dikenakan sanksi administratif berupa teguran tertulis, denda administratif, penghentian sementara, pemutusan

akses, dan/atau dikeluarkan dari daftar.

Sementara itu, sebagai perbandingan hukum, Implementing Regulation (EU) 2024/482 mengatur terkait 4 hal mengenai konsekuensi apabila tidak patuh, yakni konsekuensi terhadap ketidaksesuaian *ICT Product* atau PP yang bersertifikat; konsekuensi terhadap ketidaksesuaian oleh pemegang sertifikat; penangguhan sertifikat EUCC; dan konsekuensi dari ketidakpatuhan oleh *Conformity Assessment Body* (CAB) atau badan penilaian kepatuhan.

Pertama, berdasarkan Article 28 Implementing Regulation (EU) 2024/482 terkait konsekuensi ketidaksesuaian pada sertifikat *ICT Product* dan PP bahwa apabila sertifikat tersebut tidak sesuai, informasi ini harus disampaikan kepada pemegang sertifikat oleh lembaga sertifikasi untuk diminta identifikasi dan perbaikan dalam jangka waktu maksimal 30 hari yang nantinya akan dinilai tindakan perbaikan tersebut oleh lembaga sertifikasi. Apabila pemegang sertifikat tidak bekerja sama dengan baik atau tidak mengusulkan tindakan perbaikan dalam jangka waktu tiga puluh hari, sertifikat EUCC wajib untuk ditangguhkan ataupun ditarik. Kedua, dalam hal konsekuensi dari ketidakpatuhan oleh pemegang sertifikat berdasarkan Article 29 Implementing Regulation (EU) 2024/482 bahwa apabila lembaga sertifikasi menemukan bahwa pemegang atau pemohon sertifikat tidak mematuhi kewajiban berdasarkan peraturan tersebut dengan jangka waktu maksimal 30 hari, pemegang atau pemohon harus melakukan perbaikan, apabila tidak dilakukan, sertifikat akan ditangguhkan atau ditarik. Penarikan sertifikat tersebut terjadi apabila pelanggaran terjadi secara terus-menerus atau berulang.

Ketiga, dalam hal penangguhan sertifikat EUCC sebagaimana diatur dalam Article 30 Implementing Regulation (EU) 2024/482 bahwa penangguhan dilakukan apabila terdapat kondisi yang memicu penangguhan berdasarkan peraturan tersebut yang berlangsung maksimal 42 hari yang dimulai setelah adanya keputusan dari lembaga sertifikasi. Penangguhan tersebut harus disertai dengan alasan penangguhan, tindakan selanjutnya, dan periode penangguhan kepada pemegang sertifikat dan otoritas terkait. Selain itu, pemegang sertifikasi harus menginformasikan kepada konsumen dan masyarakat umum terkait adanya penangguhan dan alasannya, kecuali apabila terdapat informasi sensitif. Keempat, terkait

konsekuensi dari ketidakpatuhan oleh CAB berdasarkan Article 31 Implementing Regulation (EU) 2024/482 bahwa apabila CAB tidak mematuhi kewajibannya berdasarkan peraturan tersebut, wajib untuk mengidentifikasi sertifkat EUCC yang berpotensi terkena dampak, meminta evaluasi terhadap hasil sertifikasinya kepada lembaga yang lebih berwenang, menganalisis dampak ketidakpatuhan, menginformasikan kepada pemegang sertifikat yang terkena dampak. CAB harus mengambil pilihan keputusan, yaitu mempertahankan sertifikat tanpa perubahan atau menarik sertifikat tersebut.

Berdasarkan perbandingan hukum tersebut, walaupun Uni Eropa belum memberlakukan EUCC sebagai kewajiban, tetapi telah mengaturnya secara komprehensif terkait konsekuensi apabila terjadinya ketidakpatuhan terhadap peraturan tersebut dengan mengambil berbagai perspektif sebagai bentuk tindakan hukum pemerintah, seperti lembaga sertifikasinya, pemegang sertifikat, penangguhan, hingga produk sertifikasinya tersebut. Pengaturan ini memberikan perlindungan hukum sebagai akibat hukum terhadap pemegang sertifikat, konsumen, serta masyarakat umum dalam menggunakan produk TIK tersebut. Di sisi lain, Indonesia hanya mengaturnya dalam Pasal 18 yang mensyaratkan terjadinya pencabutan sertifikat dari tiga kondisi tertentu tanpa memberikan perlindungan lebih kepada konsumennya apakah diinformasikan atau tidak terkait terjadinya pencabutan tersebut. Walaupun terdapat sanksi administratif apabila tidak melakukan ketentuan Pasal 23 PP PSTE, tetapi ketentuan ini tidak merujuk langsung bentuk pengamanan terhadap perangkat keras dan lunak seperti apa yang dimaksud.

SIMPULAN

1. Indonesia dan Uni Eropa memiliki perbedaan dalam mengatur sertifikat CC untuk menjaminkan keamanan produk TIK, seperti mengklasifikasikan jenis sertifikat berdasarkan *ICT Product* dan *ICT Process*, produk tidak mengenal adanya kategori *basic* untuk jaminan keamanan sehingga memiliki jaminan keamanan yang tinggi, memiliki dua jaminan keamanan (EAL dan AVA_VAN Level), serta adanya kewajiban untuk memelihara jaminan keamanan tersebut. Sementara itu, Indonesia belum mengaturnya secara komprehensif,

seperti tidak menjelaskan lebih lanjut bagaimana jaminan keamanannya, tidak diwajibkan memelihara jaminan keamanan, memiliki konsep dan mekanisme sertifikasi yang berbeda. Dengan demikian, jaminan keamanan Indonesia lebih rendah daripada Uni Eropa.

2. Sebagai bentuk pelindungan hukum yang tepat bagi Indonesia yang dapat diadopsi dari Uni Eropa perlu untuk memperhatikan empat unsur pelindungan hukum. Unsur-unsur tersebut apabila dikaitkan dalam hal ini adalah terkait pengayoman pemerintah kepada masyarakat di Indonesia belum dilakukan secara maksimal karena masih rendahnya produk yang telah disertfikasi melalui CC, sementara di Uni Eropa walaupun belum berlaku secara efektif, tetapi telah disosialisasikan sejak pembuatan peraturan tersebut; terkait jaminan kepastian hukum di Indonesia sudah diatur melalui PBSSN 15/2019, tetapi implementasinya rendah sehingga tidak sejalan dengan tujuan atau harapan awal peraturan tersebut serta PBSSN 15/2019 lebih menitikberatkan para pihak di dalamya, sedangkan di Uni Eropa mekanismenya terarah, jelas, dan mempermudah para pihak sehingga nantinya dapat berlaku secara efektif serta peraturan tersebut juga mengatur secara seimbang antara para pihak dengan mekanisme sertifikasi; terkait hak-hak warga negara di Indonesia belum memberikan jaminan keamanan sehingga potensi adanya kejahatan siber melalui produk TIK juga masih tinggi, sementara di Uni Eropa sudah memberikan kepastian hukum kepada masyarakat Uni Eropa; dan terkait sanksi di Indonesia belum mengaturnya, sedangkan di Uni Eropa sudah dengan mencabut sertifikasi tersebut apabila tidak mematuhi peraturan tersebut serta sanksi lainnya yang diberlakukan kepada para pihak, tidak hanya dari pelaku usaha.

DAFTAR PUSTAKA

M. Ramli, Ahmad. 2010. *Cyber Law dan Haki dalam Sistem Hukum Indonesia*, Refika Aditama, Bandung.

Lessig, Lawrence. 1999. *Code and Other Laws of Cyberspace*, Basic Books, Inc., New York.

Grabowski, Mark & P. Robinson, Eric. 2022. *Cyber Law and Ethics (Regulation of the Connected World)*, Routledge, New York.

McKinsey. 2013. *Disruptive Technologies: Advances That Will Transform Life, Business, And The Global Economy*, McKinsey & Company, San Francisco.

Kusumaatmadja, Mochtar. 2006. *Konsep-Konsep Hukum dalam Pembangunan*, Alumni, Bandung.

Amirulloh, Muhamad. 2017. *Cyberlaw Perlindungan Merek dalam Cyberspace (Cybersquatting terhadap Merek)*, Refika Aditama, Bandung.

Dwi Putranto, Rahmat. 2023. *Teknologi Hukum: Paradigma Baru Hukum di Dunia Digital*, Kenacan, Jakarta.

Maruli T. Situmeang, Sahat. 2020. *Cyber Law*, CV. Cakra, Bandung.

Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

Peraturan Pemerintah Nomor 80 Tahun 2019 tentang Perdagangan Melalui Sistem Elektronik.

Peraturan Badan Siber dan Sandi Negara Nomor 8 Tahun 2020 tentang Sistem Pengamanan dalam Penyelenggaraan Sistem Elektronik.

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No. 526/2013 (EU Cybersecurity Act).

Commission Implementing Regulation (EU) 2024/482 of 31 January 2024 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC)

Halim Harahap, Abdul, (et.al.). April 2023. "Pentingnya Peranan CIA Triad Dalam Keamanan Informasi dan Data Untuk Pemangku Kepentingan atau Stakeholder," *Jurnal Manajemen dan Pemasaran Digital (JMPD)*, 1(2).

Adi, Hermawan, (et.al.). September 2022. "Analisa Keamanan Data Melalui Website Zahra Software Menggunakan Metode Keamanan Informasi CIA Triad," *Jurnal Informatika: Jurnal Pengembangan IT (JPIT)*, 7(3).

Santoso, Agus & Pratiwi, Dyah. Desember 2008. "Tanggung Jawab Penyelenggaraan Sistem Elektronik Perbankan dalam Kegiatan Transaksi Elektronik Pasca Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik," *Jurnal Legislasi Indonesia*, 5(4).

Mefford, Aron. 1997. "Lex Informatica: Foundation of Law on the Internet", Indiana Journal of Global Legal, 5(1). Artikel 11.

Napitupulu, Darmawan. 2017. "Kajian Peran Cyber Law dalam Memperkuat Keamanan Sistem Informasi," *Deviance Jurnal Kriminologi*, 1(1).

Hassanah, Hetty & Wahyudi. Juni 2021. "Prinsip-Prinsip yang Harus Dipertimbangkan dalam Penyelesaian Sengketa Nama Domain Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik," *Negara Hukum*, 12(1).

Raharjo, Ign. Sumarsono. Januari 2015. "Lex Informatica sebagai Sarana Harmonisasi Hukum dalam Electronic Commerce untuk Memperlancar Transaksi ME-ASEAN," *Prosiding Seminar Nasional (Kesiapan Indonesia: Harmonisasi Hukum Negara-Negara ASEAN Menuju Komunitas ASEAN 2015*, *Muhammadiyah University Press*.

Aji, M. Prakoso. November 2022. "Sistem Keamanan Siber dan Kedaulatan Data di Indonesia dalam Perspektif Ekonomi Politik (Studi Kasus Perlindungan Data Pribadi)," *Politica*, 13(2).

Kumar, P. Ravi, (et.al). 2018. "Exploring Data Security Issues and Solutions in Cloud Computing", *Procedia Computer Science*, No. 125.

Raihana, (et.al.). 2023. "Pengaruh Perkembangan Teknologi Terhadap Kemajuan Hukum di Indonesia," *Jurnal Pendidikan dan Konseling*, 5(2).

Alivia Sri Ananda, Safrida ,(et.al.). April 2022. "Analysis of the EU Cybersecurity Act Under the Theory of Neoliberal Institutionalism," *Arena Hukum*, 15(1).

Putranto Saptohutomo, Aryo. 2024. "PDN Diretas Pengelola Sampai Pejabat Dinilai Patut Ditindak Tegas", <https://nasional.kompas.com/read/2024/06/28/05150091/pdn-diretas-pengelola-sampai-pejabat-dinilai-patut-ditindak-tegas>, [diakses pada 02/07/2024].

Sami Bhayangkara, Chyntia. 2024. "Awas! Dampak Kebocoran Data Imbas PDN Diretas: Nama Ibu Kandung Bocor, Rekening Terancam Dibobol", <https://www.suara.com/lifestyle/2024/06/30/210817/awas-dampak-kebocoran-data-imbas-pdn-diretas-nama-ibu-kandung-bocor-rekening-terancam-dibobol>, [diakses pada 01/07/2024].

Ernis, Devy. 2024. "PDN Diretas, Anggota DPR Duga Ada Penyelewengan Dana Pemeliharaan Rp700 Miliar", <https://nasional.tempo.co/read/1885737/pdn-diretas-anggota-dpr-duga-ada-penyelewengan-dana-pemeliharaan-rp-700-miliar>, [diakses pada 01/07/2024].

Dutch NCAA. (tanpa tahun). "The Cybersecurity Act", <https://www.dutchncca.nl/the-

cybersecurityact>, [diakses pada 05/03/2024].

Fischer, Eric. 2016. "Cybersecurity Issues and Challenges: In Brief", Congressional Research Service Report, <https://sgp.fas.org/crs/misc/R43831.pdf>, hlm. 1-3, [diakses pada 11/04/2024].

IT Governance UK. (Tanpa Tahun). "The EU Cybersecurity Act", <https://www.itgovernance.co.uk/eu-cybersecurity-act>, [diakses pada 01/07/2024].

Tiofani, Krisda & Wira Widyanti, Ni Nyoman. 2024. "Kronologi Sistem Imigrasi Lumpuh Akibat Ransomware", <https://travel.kompas.com/read/2024/06/29/145111127/kronologi-sistem-imigrasi-lumpuh-akibat-ransomware>, [diakses pada 02/07/2024].

Mulyadi, Lilik. (tanpa tahun). "Teori Hukum Pembangunan Prof. Dr. Mochtar Kusumaatmadja, S.H., LL.M.", <https://badilum.mahkamahagung.go.id/upload_file/img/article/doc/kajian_deskriptif_analitis_teori_hukum_pembangunan.pdf>, [diakses pada 11/04/2024].

Amirulloh, Muhamad. 2024. "Struktur Sistem Elektronik yang Andal dan Aman", <https://blogs.unpad.ac.id/muhamadamirulloh/2024/05/08/struktur-sistem-elektronik-yang-andal-dan-aman/>, [diakses pada 07/09/2024].

Norwich University. (tanpa tahun). "The 5 Pillars of Information Assurance", <https://online.norwich.edu/online/about/resource-library/5-pillars-information-assurance>, [diakses pada 11/04/2024].

Sekretariat KADIN Indonesia. 2024. "Evaluasi Regulasi Keamanan Siber Indonesia", <https://kadin.id/info-advokasi/evaluasi-regulasi-keamanan-siber-indonesia/>, [diakses pada 05/03/2024].

Tempo.co. 2022. "Bamsoet Apresiasi Peluncuran Buku Karya Prof. Dr. Ahmad M. Ramli", <https://nasional.tempo.co/read/1649309/bamsoet-apresiasi-peluncuran-buku-karya-prof-dr-ahmad-m-ramli#:~:text=Teori%20Hukum%20Transformatif%20yang%20dicetuskan,ketertiban%2C%20kepastian%2C%20dan%20keadilan>, [diakses pada 11/04/2024].