CIVIC EDUCATION PERSPECTIVE JOURNAL

Tantangan dan Kesiapan Indonesia Menghadapi Ancaman Siber

Civic Education Perspective Journal
Vol. 5 No. 2 (2025)

online-journal.unja.ac.id/cepj/indeks

Intan Indah Megasari[1], Yasmin Humaira Azzahra[2].

[1,2]Universitas Pendidikan Indonesia, Bandung, Indonesia

***Corresponding Author*:** intanindah@upi.edu

Article Info

Article history:
Received: 17-02-2025
Revised: 15-03-2025
Accepted: 20-06-2025

Kata Kunci:
Pancasila, *Tantangan, Kesiapan Indonesia, Ancaman Siber*

Abstrak

Penelitian ini bertujuan untuk meningkatkan kesadaran dan mengambil langkah-langkah konkret, Indonesia dapat meningkatkan kesiapannya dalam menghadapi ancaman siber dan melindungi keamanan nasional di era digital. Metode penelitian yang digunakan adalah studi literatur mengkaji terhadap berbagai sumber, seperti artikel ilmiah, laporan penelitian, kebijakan pemerintah, berita media massa, dan publikasi lainnya yang relevan dengan topik penelitian. Data yang terkumpul dianalisis secara kualitatif untuk mengidentifikasi tema-tema kunci terkait tantangan dan kesiapan Indonesia dalam menghadapi ancaman siber. Hasil penelitian menunjukkan bahwa Indonesia menghadapi berbagai tantangan signifikan dalam menghadapi ancaman siber, antara lain kesenjangan kapasitas tenaga ahli yang kompeten dan terlatih, kurangnya kesadaran terhadap serangan siber, koordinasi yang lemah antar lembaga pemerintah dan sektor swasta dalam penanganan ancaman siber yang masih perlu ditingkatkan, keterbatasan anggaran yang dialokasikan untuk keamanan siber masih terbatas, dan regulasi yang belum kuat terkait keamanan siber dalam perkembangan teknologi.

Keywords:

Pancasila, Challenge, Indonesia's Readiness, Cyber Threats

Abstract

This research aims to raise awareness and take concrete steps so that Indonesia can improve its readiness to deal with cyber threats and protect national security in the digital era. The research method used is a literature study reviewing various sources, such as scientific articles, research reports, government policies, mass media news, and other publications relevant to the research topic. The data collected was analyzed qualitatively to identify key themes related to Indonesia's challenges and readiness in facing cyber threats. The results showed that Indonesia faces various significant challenges in dealing with cyber threats, including gaps in the capacity of competent and trained experts, lack of awareness of cyber attacks, weak coordination between government agencies and the private sector in handling cyber threats that still need to be improved, limited budget allocated for cyber security is still limited, and regulations that are not yet strong related to cyber security in technological developments

Pendahuluan

Meningkatnya penggunaan Internet telah membuka pintu baru bagi beberapa orang yang paham perangkat komputer serta adanya celah untuk secara tidak tepat menggunakan teknologi ini untuk kegiatan kriminal yang merugikan orang lain. Pertumbuhan pesat teknologi digital dan Internet ini memang memiliki dua sisi yaitu sisi positif dan sisi negatifnya, yang mana hal ini signifikan. Pertama, sisi positif dari Internet adalah memudahkan dalam melakukan berbagai aktivitas sehari-hari, meningkatkan ketersediaan informasi, dan mendorong kreativitas dalam beberapa aspek. Namun perkembangan teknologi gelombang baru ini patut diwaspadai karena juga mempunyai sisi negatifnya, terutama munculnya bentuk-bentuk kejahatan baru yang belum pernah dialami sebelumnya.

Informasi teknologi sangat bermanfaat bagi kehidupan manusia, tetapi juga hasil perkembangan informasi teknologi yang dapat disalahgunakan oleh oknum tertentu. Internet memungkinkan terjadinya kejahatan yang bersifat tradisional menjadi kejahatan modern yang cakupannya lebih luas dan risiko kerugiannya lebih besar.

Pembobolan atau peretasan, penipuan online, pencurian identitas, dan penyebaran informasi palsu adalah beberapa bentuk kejahatan dunia maya yang paling umum dan tidak berdasar yang dilakukan saat ini. Ekspansi global yang dimiliki para pelaku kejahatan siber seringkali menjadi sarana bagi mereka untuk melakukan aksinya, sehingga kejahatan siber memiliki dampak yang bersifat global dan lebih sering menjadikan proses hukum menjadi kompleks. Dengan tersedianya internet di hampir semua aspek kehidupan, batas ruang dan waktu tidak lagi menjadi kendala. Masyarakat umum menganggap perkembangan pesat pemanfaatan jasa internet sebagai hal yang lumrah. Namun, situasi ini dikendalikan oleh kemudahan kejahatan. Yang mana diistilahkan sebagai *cybercrime.* Secara sederhana cybercrime adalah istilah yang mengacu kepada aktivitas kejahatan dengan komputer atau jaringan komputer menjadi alat, sasaran atau tempat terjadinya kejahatan. (Sulisrudatin, 2018). Di sisi lain, Negara Indonesia yang memiliki jumlah penduduk peringkat empat di dunia juga tidak terlepas dari hal ini. Indonesia menyumbang 2,4% kejahatan siber dunia. Angka ini naik 1,7% dari tahun 2010 ketika Indonesia menduduki peringkat ke-28. Hal ini dapat dikaitkan dengan perubahan perilaku konsumen sehubungan dengan penggunaan internet di Indonesia yang meningkat pada tingkat yang mengkhawatirkan (Suhaemin, 2023).

Berangkat dari beberapa penelitian sebelumnya, diantaranya peran literasi digital dalam penguatan profil pelajar Pancasila dimensi mandiri, bernalar kritis, dan kreatif, dimana literasi digital menjadi hal yang penting dalam pendidikan, terutama di dalam pengembangan profil pelajar Pancasila, dari hasil penelitiannya, literasi digital memiliki peranan yang signifikan dalam menguatkan dan mengembangkan profil pelajar Pancasila (Santoso & Adha, 2019; Santoso & Wuryandani, 2020). kemudian penelitian sebelumnya ada, ancaman *cybercrime* di Indonesia sebuah tinjauan pustaka sistematis, temuan penelitian menunjukkan bahwa telah terjadinya evolusi publikasi tentang *cybercrime* di Indonesia dari fokus awal pada pemahaman dan regulasi hingga penekanan yang lebih besar pada teknologi, ancaman terbaru, dan dampaknya terhadap berbagai aspek kehidupan dan bisnis, serangan *cybercrime* di Indonesia tergolong serius karena berpotensi tinggi menimbulkan permasalahan nasional (Anggraeny et al., 2022; Fadhillah et al., 2023; Hartono et al., 2021; Lubis, 2022; Nyoman Juwita Arsawati et al., 2021; Rosy, 2020; Silalahi et al., 2023).

Kemudian ada, analisa kasus *cybercrime* bidang perbankan berupa modus pencurian data kartu kredit, di dunia perbankan berkembangnya kejahatan yang lebih canggih yang dikenal *cybercrime*, diantaranya oleh pelaku kejahatan perbankan untuk tujuan pencurian data kartu kredit para nasabah (Fitri, 2021; Goni, 2021; Goni et al., 2022; Ivanyuk, 2024; Nayar & Rathod, 2021). Atas dasar beberapa penelitian sebelumnya, peneliti tertarik untuk mengembangkan pentingnya literasi siber dengan penguatan nilai Pancasila, agar menjadi warga negara yang cerdas dan bertanggung jawab dalam pengelolaan digital . Dengan berkembangnya teknologi informasi dan komunikasi (TIK), negara berada di bawah tekanan yang signifikan untuk membangun kemampuan yang kuat untuk memahami potensi teknologi digital dan membuat rencana pengarusutamaan yang sesuai dengan tujuan kebijakan jangka pendek dan jangka panjang.

Berbicara tentang peran pemerintah dalam pembangunan, hukum tentunya memiliki

kedudukan yang sangat berperan, untuk tidak hanya mendorong pelaksanaan pembangunan nasional tetapi juga untuk menjaga pencapaian yang telah dicapai, di antaranya adalah perlindungan hak atas kebebasan berekspresi dan pemberantasan kejahatan dunia maya (Beduschi, 2019; Bellanova, 2017; Chen & Miao, 2023; Fabbrini & Celeste, 2020; Floridi, 2018; He, 2022; Romansky, 2022; Yuspin et al., 2023). Terkait dengan *cybercrime*, tantangannya bahkan lebih besar mengingat fakta bahwa sebagai manifestasi globalisasi, *cybercrime* merupakan kejahatan transnasional tanpa batas dan karenanya sulit untuk diberantas atau dikendalikan dari lokasi mana pun. *Cybercrime* memengaruhi individu tetapi terutama organisasi baik pemerintah maupun non-pemerintah dan akibatnya menimbulkan ancaman terhadap tatanan ekonomi dan sosial negara. Oleh karena itu, hukum harus mampu menanggapi perubahan cepat dalam lingkungan digital dan juga cukup melindungi pengguna internet di semua sektor.

Manfaat dari penulisan ini sangat signifikan, terutama bagi pengguna internet yang semakin beragam. Dengan mempelajari tindakan yang dilakukan oleh para penjahat dunia maya dalam sistem digital, kita dapat lebih berhati-hati dan waspada saat menggunakan internet. Hal ini juga memungkinkan kita untuk mengidentifikasi tanda-tanda dan pola yang biasanya ditampilkan oleh para penjahat dunia maya, sehingga memungkinkan kita untuk mengambil tindakan perlindungan yang diperlukan guna melindungi diri kita dan informasi Kita, serta menguatkan diri dengan mengaplikasikan nilai-nilai Pancasila dalam kehidupan sehari-hari.

Metode

Dalam penulisan artikel ini, penulis menggunakan rujukan dari M. Sari dan Asmendri dalam menggunakan metode penelitian (studi kepustakaan) untuk mendapatkan informasi data. Menurut M. Sari dan Asmendri dalam Indarta et al. (2022), penelitian yang menggunakan metode ini mendapatkan informasi data dari berbagai sumber, termasuk buku dan artikel jurnal yang relevan dengan masalah yang akan dibahas. Dalam hal ini, peneliti mengumpulkan informasi dari buku, jurnal, catatan, membaca, dan mencatat, serta mengolah bahan penelitian yang terkait secara mendalam bagaimana literasi siber di Indonesia dapat dibangun dan diperkuat dengan mengintegrasikan nilai-nilai Pancasila, demi meningkatkan kesiapan nasional dalam menghadapi berbagai ancaman digital.

Dengan mengkaji berbagai literatur yang relevan mulai dari jurnal ilmiah, buku, laporan penelitian, hingga dokumen kebijakan pemerintah studi ini berupaya mensintesis informasi komprehensif mengenai konsep literasi siber, urgensi keamanan siber di era modern, serta peran fundamental Pancasila sebagai landasan filosofis dan etis bagi warga negara digital Indonesia. Data sekunder yang terkumpul akan dianalisis secara kualitatif untuk mengidentifikasi tema-tema kunci terkait tantangan yang dihadapi Indonesia, seperti kesenjangan kapasitas sumber daya manusia, kurangnya kesadaran, koordinasi antar lembaga yang belum optimal, keterbatasan anggaran, dan kerangka regulasi yang masih perlu diperkuat. Melalui analisis ini, penelitian ini bertujuan untuk merumuskan strategi yang adaptif dan holistik dalam menumbuhkan kesadaran serta partisipasi aktif masyarakat dalam menjaga keamanan siber, sesuai dengan nilai-nilai luhur Pancasila (Sari, 2020).

Hasil dan Pembahasan

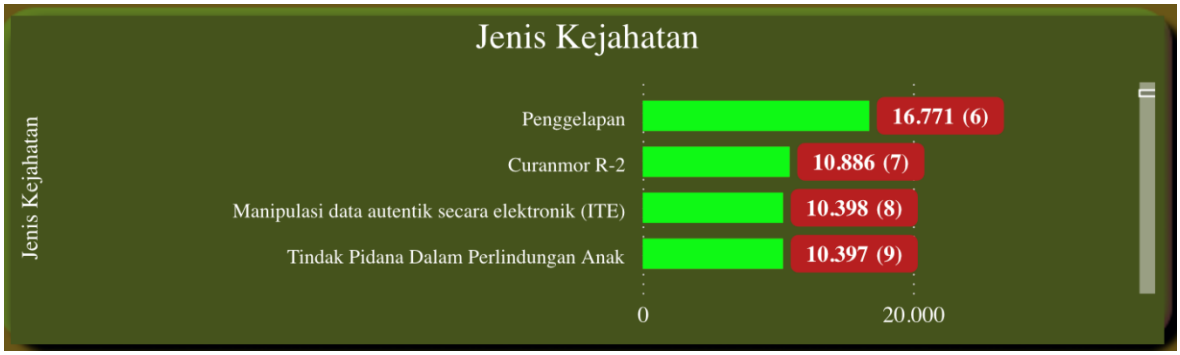
Kejahatan siber atau *cybercrime*, secara sempit merefer kepada kejahatan yang berarsitektur pada sistem tertentu (Ambika & Senthilvel, 2020; Broadhurst et al., 2014; Dm et al., 2022; Maimon & Louderback, 2019; Suharto & Maria Novita Apriyani, 2021; Timofeyev & Dremova, 2022). Sedangkan secara luas *cybercrime* merupakan segala kejahatan baru yang meneriakan sasaran pada komputer atau jaringan komputer dan pengguna arus informan tersebut. Kejahatan *cybercrime* juga mencakup kejahatan konvensional yang melibatkan teknologi informasi dan komputer dan disebut sebagai kejahatan terkait komputer. Oleh karena itu, kejahatan *cybercrime* mencakup setiap kegiatan ilegal yang berkaitan dengan penggunaan komputer atau jaringan komputer, atau yang berkaitan dengan jaringan komputer, atau yang dilakukan terhadap jaringan komputer.

Menurut Hapsari (2018), *Cybercrime* dapat didefinisikan sebagai kejahatan yang berkaitan dengan kepentingan pribadi atau kelompok tertentu. Banyak orang, baik secara langsung maupun tidak langsung, menggunakan teknologi untuk memperluas jangkauan kejahatan *cybercrime*. Seringkali, berbagai kepentingan, termasuk agama, politik, ekonomi, dan budaya, menunjukkan, mendorong, atau bahkan membenarkan seseorang atau sekelompok individu sebagai pelaku kejahatan siber. Motivasi ini menciptakan lingkungan dimana kejahatan dapat terjadi dengan mengembangkan sistem informasi dan komunikasi yang sudah ada (Hapsari & Pambayun, 2023).

Cybercrime maya adalah kejahatan yang terjadi ketika ada komunitas di dunia maya, khususnya di internet, dan memiliki karakteristik khusus yang membedakannya dari kejahatan biasa. Pertama, jenis kejahatan ini dilakukan di dunia maya, tempat tindakan ilegal, tidak sah, atau tidak bermoral terjadi, sehingga sulit untuk menentukan yurisdiksi yang tepat. Kedua, tindakan kriminal ini dilakukan melalui perangkat yang terhubung ke internet. Ketiga, jenis kerugian yang biasanya ditimbulkannya biasanya lebih besar, baik secara nyata maupun tidak nyata, termasuk, tetapi tidak terbatas pada, waktu, nilai, layanan, uang, barang, harga diri, martabat, informasi pribadi, dan banyak lagi. Selain itu, pelaku kriminal jenis ini biasanya mahir menggunakan internet dan aplikasinya. Terakhir, kejahatan semacam ini biasanya melibatkan beberapa negara, melintasi batas negara, membuat penegakkan hukum lebih sulit. (Amin Suhaemin, 2023).

Statistik kasus cybercrime di Indonesia sedang mengalami peningkatan yang cukup banyak. Pada tahun 2022, pemapat kebangkan kejahatan siber lebih jauh dengan Bareskrim

Polri telah memproses seluruh 8831 kasus, yang sebagian besar melibatkan 8372 orang sebagai tersangka yang dilaporkan. Pada tahun 2023, laporan kasus kejahatan dunia maya dari berbagai wilayah di negara ini mencapai proporsi yang mengkhawatirkan dengan terdapat pada daerah tangerang mencatat angka tertinggi yaitu 1.472 kasus; sepanjang tahun itu, lebih dari 38.563 laporan aktivitas kriminal terkait dunia maya telah terdeteksi. (detiklnet, 2023).



Sumber : https://pusiknas.polri.go.id/data_kejahatan

Gambar 1. Data Kejahatan dari periode 1 Januari 2025 s/d 30 Juli 2025

Dari data diatas digambarkan bahwa kejahatan manipulasi data periode 1 Januari s/d 30 Juli 2025 menempati peringkat yang cukup tinggi dalam artian, masih cukup banyak pelanggaran yang terjadi disekeliling kita kejahatan *cyber*. Hal ini menimbulkan rasa geram karena mayoritas penyelewengan data ini tidaklah diketahui secara pasti oleh korban, maka dari hal ini perlunya pendekatan pengetahuan dan penguatan nilai Pancasila untuk meminimalisir kejadian kejahatan serupa. Dampak kejahatan *cybercrime* terhadap masyarakat dan ekonomi sangat serius. Dengan lebih dari 97 juta akun di Indonesia yang dilaporkan menjadi korban pelanggaran data sejak tahun 2020 hingga 2024, masalah keamanan siber menjadi perhatian utama bagi konsumen dan pelaku bisnis. Kejahatan ini tidak hanya menimbulkan dampak material, tetapi juga menimbulkan kerugian immaterial seperti hilangnya reputasi, pengkhianatan, dan penderitaan psikologis korban. (Arifin, 2019).

Pendapat dari Muqsuth dari hasil surveynya dalam jurnalnya “Survei Bela Negara mengukur sejauh mana kondisi keamanan nasional saat ini sesuai dengan cita-cita UUD 1945 dan Konstitusi kita untuk memajukan kemerdekaan dan kedaulatan negara: 58,7% menilai cukup, 30,5% menilai cukup, 7,4% menilai sangat buruk.” (Muqsith et al., 2022). Dari survei ini kepuasan tingkat aspek demokrasi ini perlu di targetkan untuk meningkatkan tingkat kepuasan terhadap demokrasi. Atas dasar ini pentingnya kontrol pemerintah untuk mendukung nilai-nilai Pancasila yaitu kebijaksanaan lokal dalam pengembangan Identitas nasional Indonesia untuk memperkuat kemanan nasional.

Ekonomi juga menjadi aspek yang akan terpengaruh, di mana kejahatan siber mempengaruhi proses bisnis, menambah biaya menjalankan bisnis pada keamanan yang ditingkatkan, serta rendahnya tingkat kepercayaan investor dan konsumen dalam bertransaksi daring. Di Indonesia, sebagian besar organisasi teori konspirasi menganggap kejahatan siber sebagai salah satu ancaman utama, banyak dari mereka berpendapat bahwa mereka telah menderita kerugian karena serangan siber. Hal ini menunjukkan perlunya peningkatan keamanan dan kewaspadaan terhadap ancaman di dunia maya (Amarini, 2018)

Menilai penggunaan sistem hukum di Indonesia sebagai salah satu cara yang digunakan untuk mengekang kejahatan sosial tertentu tampaknya tidak menimbulkan masalah mendasar. Sebagian besar termasuk evolusi hukum yang selama bertahun-tahun menunjukkan bahwa penerapan hukum pidana dalam kebijakan pemerintah pembuat hukum

merupakan hal yang melekat pada kekaisaran Romawi kuno. Oleh karena itu, penerapan hukum pidana telah diterima sebagai kegiatan biasa, yang berarti bahwa dalam kondisi seperti itu situasinya telah dianggap wajar (Indah & Sari, 2021). Sistem hukum harus berkembang untuk lebih mencerminkan komitmen Pancasila terhadap keadilan, mengadvokasi reformasi hukum pidana untuk memastikan proses yang lebih adil dan transparan (Elfrida Herawati Siregar, 2024).

"Pancasila merupakan pedoman sikap dan tindakan yang dituangkan dalam undang-undang, peraturan pemerintah, keputusan presiden, dan sebagainya. "Tidak ada bangsa yang dapat mencapai kebesarannya jika bangsa itu tidak meyakini sesuatu dan jika apa yang diyakininya tidak memiliki dimensi moral untuk menopang peradaban yang besar. Inilah pentingnya Pancasila sebagai dasar ideologi, yaitu gagasan yang mengarah pada penemuan pengetahuan atau teori. Selain itu, dengan meyakini dan membangun kepercayaan pada suatu bangsa, Pancasila juga bertujuan untuk meningkatkan potensi tujuan pembangunan. Selain itu, Pancasila, sebagai dasar negara, telah menjadi kekuatan yang berbasis pada kekuatan sosial, yaitu perjuangan rakyat Indonesia" (Muqsith et al., 2022; Sulisrudatin, 2018). Negara Indonesia memiliki dasar negara yang mengarah kedalam penemuan pengetahuan atau teori serta pembanguan kepercayaan pada suatu bangsa, maka Pancasila di jadikan sumber dari segala sumber hukum di Indonesia. Prinsip-prinsip Pancasila tentang keadilan dan kemanusiaan telah menjadi hal yang krusial dalam pengembangan kerangka kerja hak asasi manusia Indonesia.

Relevansi merefleksikan Pancasila sebagai landasan ideologis dan identitas kolektif Indonesia muncul dari kenyataan bahwa suatu bangsa hanya dapat bertahan hidup melalui semangat (Geist)-nya yang menyatukan seluruh entitas di dalamnya. Pancasila perlu diinterpretasikan ulang agar relevan dalam konteks globalisasi yang kompleks dan dinamis, serta berbagai ketegangan dan konflik sosial yang mengikutinya. Indonesia harus beradaptasi dengan perubahan-perubahan ini agar dapat memelihara dan memperkuat persatuan masyarakatnya yang majemuk. Pancasila menyediakan landasan filosofis yang berdaya untuk memfasilitasi proses adaptasi ini. (Madung & Stefanus, 2021). Penekanan Pancasila pada keadilan sosial dan kemanusiaan sejalan dengan meningkatnya seruan akan kerangka hukum yang melindungi lingkungan hidup dan menjamin pembangunan berkelanjutan (Hadiprabowo, 2024).

Kitab Undang-Undang Hukum Pidana (KUHP) Indonesia. Meskipun demikian, definisi tindak pidana dalam KUHP Indonesia sebagian besar masih konvensional dan belum sepenuhnya membahas masalah kejahatan dunia maya. Terkait hal ini, terdapat beberapa undang-undang dan peraturan yang berlaku tentang tindak pidana yang berkaitan dengan komputer menurut (Moeljatno, 2021). *KUHP (Kitab undang-undang hukum pidana)*, seperti berikut ini:

1. Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi, yang mengatur tentang penyelenggaraan dan pengelolaan layanan telekomunikasi.
2. Undang-Undang Nomor 19 Tahun 2002 tentang Hak Cipta, yang melindungi karya-karya cipta, termasuk yang dihasilkan secara digital.
3. Undang-Undang Nomor 25 Tahun 2003 tentang Perubahan atas Undang-Undang Nomor 15 Tahun 2002 mengenai Tindak Pidana Pencucian Uang, yang mencakup pengaturan terkait pencucian uang yang dapat terjadi melalui transaksi elektronik.
4. Undang-Undang Nomor 15 Tahun 2003 tentang Pemberantasan Tindak Pidana Terorisme, yang mencakup aspek kejahatan siber yang berkaitan dengan terorisme.

5. Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, yang merupakan landasan hukum utama untuk mengatur kegiatan di dunia maya dan perlindungan data pribadi.

Peraturan perundang-undangan ini bertujuan agar hukum Indonesia dapat mengikuti perkembangan teknologi informasi dan faktor-faktor yang menyebabkan hukum di negara ini sulit untuk ditegakkan. Meskipun demikian, masih diperlukan revisi dan penyempurnaan terhadap peraturan perundang-undangan yang ada agar lebih spesifik dan menyeluruh terkait dengan kejahatan di dunia maya.

Perubahan zaman juga menuntut adanya pengaturan terhadap kegiatan di ruang *cybercrime* dan kejahatan *cybercrime* yang telah melahirkan berbagai undang-undang seperti undang-undang tentang kejahatan teknologi informasi yang tertuang dalam Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Harapan ini didasarkan pada kenyataan bahwa Undang- Undang ITE akan digunakan sebagai kekuatan kontrol dalam menjaga ketertiban dalam kegiatan pemanfaatan teknologi informasi (Indah & Sari, 2021).

Tindakan *cybercrime* diatur dalam Undang-Undang Nomor 19 Tahun 2016 tentang Pengubahan Undang-Undang Nomor 11 Tahun 2008, khususnya mengenai kesusilaan, tercantum dalam Pasal 27 ayat (1). Di dalam pasal ini diatur mengenai pengertian tentang kesusilaan, ancaman yang dipidana bagi siapa pun, yang melakukan secara sengaja dan melawan hukum, menyiarkan, mentransmisikan atau melakukan akses terhadap *wievera* elektronik dan/atau dokumen elektronik yang memiliki isi yang menentang kesusilaan. Meskipun demikian, pasal ini tidak menjelaskan secara tegas mengenai apa yang dimaksud dengan muatan yang berisi hal-hal yang tidak pantas sehingga hal ini menjadi masalah hukum yang tidak jelas mengenai hal lain yang termasuk ke dalam kategori tersebut. Ketidakjelasan seperti ini bisa jadi akan membuat pembuktian unsur-unsur tindak pidana ini serta memberikan kemungkinan lainnya tentang makna tindakan yang dianggap melanggar kesopanan di dunia maya (Moeljatno, 2021).

Indonesia telah membuat kemajuan penting dalam memerangi tantangan kejahatandunia maya, termasuk mendirikan Badan Siber dan Sandi Negara (BSSN). BSSN bertugas meningkatkan strategi keamanan dunia maya dan sebagai hasilnya bertanggung jawab untuk mengamankan data, informasi, dan transaksi elektronik yang relevan di dunia maya. BSSN juga mengoordinasikan berbagai kementerian dan lembaga sebagai bagian dari strategi Keamanan Siber Nasional dengan menerapkan langkah-langkah untuk melindungi sumber daya informasi sensitif dari akses yang tidak sah dan meningkatkan kemampuan lembaga penegak hukum dalam menangani insiden keamanan dunia maya (Sudarmadi, 2019).

Jika menelaah tentang keamanan siber di Indonesia, ada beberapa serangan siber maupun perang siber yang pernah terjadi dengan pihak lain. Pada tahun 1998 dimana kerusuhan rasial di dunia siber atau dunia maya yaitu Indonesia berperang dengan para *hacker* yang diduga dari China dan Taiwan. Di antara sepuluh negara yang mengalami serangan worm Stuxnet, Indonesia berada di urutan kedua setelah Iran, menurut penelitian yang dilakukan oleh Symantec, produsen antivirus Norton, pada Agustus 2010. (Chotimah, 2019). Hal ini perlunya antisipasi dari pihak pemerintah untuk mampu memperkuat keamanan siber agar tidak ada terulang kembali data rahasia negara yang di sadap oleh

negara lain, Menurut Barrinha dan Renard, diplomasi siber (*cyber diplomacy*) merupakan merupakan diplomasi yang dilakukan di dunia maya, baik bilateral maupun multilateral, di mana sumber daya diplomatik dan kinerja fungsi diplomatik digunakan untuk menjaga kepentingan negara di dunia maya. Dalam hal ini, agenda diplomatik yang paling penting mencakup masalah keamanan internet, kejahatan cyber,(Barrinha & Renard, 2017). Upaya peningkatan kepercayaan, kebebasan internet, dan pemerintahan internet. diplomasi ini berkembang pesat dalam menyelesaikan jenis-jenis konflik yang hadir didunia maya, upaya dialog atar pemangku kepentigan merupakan jalan untuk meraih kesepakatan dan keuntungan bersama (Prakoso, 2024).

Selama ini, keamanan internet Indonesia diawasi oleh Tim Penanganan Kejadian Keamanan Internet Infrastruktur Indonesia (IDSIRTII), Tim Penanganan Kejadian Keamanan Komputer Indonesia (ID-CERT), dan Sub Direktorat Cyber Crime Direktorat Tingkat Pidana Ekonomi dan Khusus (Dittipideksus) Bareskrim Polri, selain Undang-Undang ITE. Meskipun UU ITE menetapkan kebijakan keamanan siber, Indonesia juga menghadapi masalah menentukan siapa yang bertanggung jawab menangani kejahatan siber, terrorism siber, hacktivism siber, dan perang siber.Upaya pemerintah juga termasuk pengembangan instrumen hukum yang komprehensif untuk mendukung perlindungan data pribadi, seperti Rancangan Undang-Undang Pelindungan Data Pribadi (RUU PDP) (Hisbulloh, 2021). Dengan adanya undang-undang ini, diharapkan akan tercipta kerangka hukum yang lebih kuat untuk melindungi privasi dan data individu di era digital, sehingga dapat meningkatkan kepercayaan masyarakat terhadap penggunaan teknologi informasi. Selain itu, adanya tim tanggap darurat dan koordinasi antara berbagai pihak terkait diharapkan dapat mempercepat respons terhadap kebocoran data dan serangan siber, sehingga meningkatkan tata kelola data di Indonesia. (Bukit & Ayunda,2022).

Strategi keamanan nasional siber dan program jangka pendek dan panjang telah dimulai oleh pemerintah Indonesia untuk menghadapi tantangan di dunia maya. Teknologi adalah bidang yang terus berkembang. Kemajuan yang konstan ini telah menghasilkan beragam kelompok penjahat siber yang mengadaptasi teknik, taktik, dan protokol baru dengan kecepatan yang signifikan. Memahami para penjahat ini membutuhkan upaya penelitian yang berkelanjutan. Tipologi peretas yang diusulkan dua dekade lalu mungkin tidak cukup mencerminkan penjahat siber saat ini, sama seperti tipologi yang dikembangkan saat ini mungkin kurang relevan dengan penjahat siber yang terus berkembang di masa depan.(Rao et al., 2024). Namun, ada beberapa masalah dan hambatan yang cukup besar saat menerapkannya dalam praktik. Pertama, dari sudut pandang sumber daya manusia, masih ada kekurangan karyawan yang berpengalaman dan terampil dalam keamanan siber. Selain itu, hal ini membuat upaya untuk membuat dan menerapkan strategi dan tindakan perlindungan infrastruktur digital yang tepat menjadi sulit. Selain itu, pelaksanaan dan pelaksanaan kebijakan bantuan pencegahan juga menghadapi kesulitan, terutama dalam hal koordinasi antar pemangku kepentingan. Untuk mewujudkan ekosistem yang sehat, tidak hanya pemerintah dan sektor swasta, tetapi juga lembaga dan masyarakat internasional harus bekerja sama lebih banyak dalam pengembangan aplikasi.

Sangat penting bagi masyarakat untuk berpartisipasi dalam pencegahan kejahatan siber, terutama dalam hal meningkatkan kesadaran terhadap keamanan digital dan langkah-langkah yang harus diambil untuk mengurangi ancaman yang mungkin muncul. Diantaranya (1) Peningkatan sistem keamanan data, (2) Edukasi dan sosialisasi keamanan siber, (3) Penerapan enkripsi dan proteksi data, (4) Kolaborasi dengan pihak keamanan siber, (5) Pengawasan dan penanganan insiden siber. (Diskominfo, 2025). Strategi komprehensif

untuk memerangi kejahatan siber melibatkan langkah-langkah teknologi seperti pembaruan perangkat lunak dan enkripsi, kampanye edukasi dan kesadaran, legislasi yang kuat, dan kerja sama internasional.(Gundu et al., 2025). Masyarakat adalah garda terdepan dalam mengidentifikasi dan menangani serangan siber. Mengetahui tentang risiko dan strategi penanggulangan kejahatan siber dapat sangat membantu mengurangi jumlah kejahatan siber yang terjadi. Negara dan organisasi swasta dapat melakukan berbagai upaya untuk meningkatkan kesadaran publik tentang masalah keamanan siber. Misalnya, pelatihan tentang penggunaan kata sandi yang kuat, pengenalan *phishing*, dan perlindungan data pribadi dapat membantu dalam mengajarkan orang tentang cara melindungi diri mereka sendiri saat menggunakan internet. Dengan mengintegrasikan AI dengan langkah-langkah keamanan siber, kerangka kerja ini memfasilitasi identifikasi dan prediksi dini tingkat kejahatan, memberdayakan lembaga penegak hukum dan pembuat kebijakan dengan wawasan yang dapat ditindaklanjuti untuk secara proaktif mengatasi ancaman yang muncul (Rao et al., 2024). Perlunya pelatihan untuk memperkuat stabilitas dengan menguasai aplikasi-aplikasi seperti AI untuk memperkuat keamanan siber.

Simpulan

Pemerintah Indonesia terlebih lagi telah melakukan berbagai langkah untuk mengurangi risiko kejahatan siber, termasuk kebijakan dan pembentukan badan seperti Badan Siber dan Sandi Negara (BSSN). Namun tantangannya masih cukup besar, antara lain kurangnya tenaga terampil di bidang keamanan siber, kebutuhan untuk memperbarui undang- undang yang lebih responsif terhadap kemajuan teknologi, dan kesulitan dalam kolaborasi antar pemangku kepentingan. Pembaharuan pengalaman dan pengetahuan dari para lembaga sangatlah berperan, mengingat proses perkembangan teknologi yang sangat cepat serta penyebaran data yang sangat masif, hal ini perlu dinilai penting oleh negara.

Dari sudut pandang strategis dalam menangani permasalahan tersebut, pemerintah perlu memperkuat kerangka hukum yang ada, meningkatkan investasi pada keamanan, dan

yang terpenting mendidik dan menyadarkan masyarakat agar mereka dapat menjadi bagian dari solusi masalah tersebut. Dengan langkah-langkah tersebut, diharapkan bahwa keberhasilan dalam memerangi kejahatan dunia maya akan meningkat untuk mengekang risiko yang terus meningkat yang ditimbulkan oleh dunia maya kepada warga negara. Kebutuhan akan kolaborasi dan koordinasi multi-sektoral yang berkelanjutan antara pemerintah, sektor swasta, dan masyarakat luas merupakan hal yang penting untuk mengembangkan lingkungan yang aman dan tangguh terhadap setiap kejadian kejahatan dunia maya dan penggunaan teknologi informasi tanpa rasa takut dari masyarakat. Penting untuk meningkatkan pelatihan dan pendidikan bagi para penegak hukum dan praktisi di bidang keamanan dunia maya. Hal ini dapat dicapai melalui keterlibatan lembaga pendidikan, organisasi internasional, dan sektor swasta dalam menyediakan pelatihan dan

sertifikasi yang sesuai.

Paduan teknologi dan penyuluhan pencegahan kejahatan siber merupakan teknologi

yang khusus dikembangkan untuk menanggulangi ancaman siber. Pemanfaatan teknologi seperti AI juga terbilang penting untuk proses identifikasi dan prediksi dini tingkat kejahatan, memberdayakan penegak hukum dengan wawasan yang dapat ditindaklanjuti. Kampanye kesadaran publik tentang keamanan siber dan praktik perlindungan diri dari

ancaman seharusnya diprakarsai oleh pemerintah. Dengan memahami risiko dan stratego penganggulangan, masyarakat dapat menjadi garda terdepan dalam mengurangi jumlah kejahatan siber yang terjadi. Singkatnya, pengembangan mekanisme yang bermakna untuk arus informasi dan praktik dalam memerangi kejahatan siber di antara pemerintah, sektor swasta, organisasi internasional, dan masyarakat sipil sangatlah penting.

Referensi

Andysah P,U, Siahaan. (2018) Pelanggaran Cybercrime Dan Kekuatan Yurisdiksi Di Indonesia, Jurnal Teknik Dan Informatika,Vol.5 No.1 Januari 2018, https://jurnal.pancabudi.ac.id/index.php/Juti/article/view/82

Amarini, I. (2018). *Pencegahan Dampak Negatif Perkembangan Teknologi Informasi Terhadap Pengguna Internet*. Jurnal Kosmik Hukum, Vol. 18 No. 1 Januari 2018 ISSN 1411-9781 .

Ambika, T., & Senthilvel, K. (2020). Cyber Crimes against the State: A Study on Cyber Terrorism in India. *Webology*, *17*(2). https://doi.org/10.14704/WEB/V17I2/WEB17016

Anggraeny, I., Monique, C., Puspitasari Wardoyo, Y., & Bhirini Slamet, A. (2022). The Urgency of Establishing Guidelines for Handling Cybercrime Cases in the Indonesian National Police Department. *KnE Social Sciences*. https://doi.org/10.18502/kss.v7i15.12107

Amin Suhaemin, M. (2023). Karakteristik Cybercrime Di Indonesia. *Journal of Islamic Law and Yurisprudance*, Volume 5, Nomor 2 (2023) Pages 15–26.

Arifin, F. R. (2019). Kajian Hukum Pidana Pada Kasus Kejahatan Mayantara (Cybercrime) Dalam Perkara Pencemaran Nama Baik Di Indonesia. *Resman Jurnal Hukum*, Volume 5, Nomor 1, April 2019, Hlm. 21-39 .

Barrinha, A., & Renard, T. (2017). Cyber-diplomacy: the making of an international society in the digital age. *Global Affairs*, *3*(4–5), 353–364. https://doi.org/10.1080/23340460.2017.1414924.

Bukit, A. N., & Ayunda, R. (2022). Urgensi Pengesahan RUU Perlindungan Data Pribadi

Terhadap Perlindungan Kebocoran Data Penerimaan SMS Dana Cepat. *Reformasi Hukum*, *26*(1), 1-20. detiklnet. (2023, November 24). *Statistik Kejahatan Siber di Indonesia Selama 2023*. Retrieved from inet.detik.com: https://inet.detik.com/security/d-7054249/statistik-kejahatan- siber-di-indonesia-selama-2023

Beduschi, A. (2019). Digital identity: Contemporary challenges for data protection, privacy and non-discrimination rights. In *Big Data and Society* (Vol. 6, Issue 2). https://doi.org/10.1177/2053951719855091

Bellanova, R. (2017). Digital, politics, and algorithms: Governing digital data through the lens of data protection. *European Journal of Social Theory*, *20*(3). https://doi.org/10.1177/1368431016679167

Broadhurst, R., Grabosky, P., Alazab, M., & Chon, S. (2014). Organizations and cyber crime: An analysis of the nature of groups engaged in cyber crime. *International Journal of Cyber Criminology*, *8*(1).

Chen, W., & Miao, L. (2023). Urban Digital Transformation and Enterprise Personal Data Protection. *Journal of Circuits, Systems and Computers*, *32*(11). https://doi.org/10.1142/S0218126623501803

Chotimah, H. C. (2019). Tata Kelola Keamanan Siber dan Diplomasi Siber Indonesia di Bawah Kelembagaan Badan Siber dan Sandi Negara Cyber Security Governance and Indonesian Cyber Diplomacy by National Cyber and Encryption Agency. *Riwayat Artikel Diterima*, *10*(2). https://doi.org/10.22212/jp.v10i1.1447

Damar Apri Sudarmadi, A. J. S. R. (2019). Strategi Badan Siber dan Sandi Negara (BSSN) Dalam Menghadapi Ancaman Siber di Indonesia. *Jurnal Kajian Stratejik Ketahanan Nasional*, *2*(2). https://doi.org/10.7454/jkskn.v2i2.10028

Dm, M. Y., Addermi, & Lim, J. (2022). Kejahatan Phising dalam Dunia Cyber Crime dan Sistem Hukum di Indonesia. *Jurnal Pendidikan Dan Konseling*, *4*(5).

Diskominfo, (2025). Tantangan Cyber Crime di 2025: Bagaimana Masyarakat Bisa Lebih Aman di Ruang Digital? https://diskominfo.bandung.go.id/detail-berita/tantangan-cyber-crime-di-2025-bagaimana-masyarakat-bisa-lebih-aman-di-ruang-digital Diakses pada 30 Juli 2025, 13:05 WIB.

Elfrida Herawati Siregar, C. B. U. M. S. (2024). Pancasila in the Context of Indonesian Legal Reform: A Critical Evaluation and International Debate. *Journal of Law and Legal Reform*, *5*(4), 2093–2126. https://doi.org/10.15294/JLLR.V5I4.18923

Fabbrini, F., & Celeste, E. (2020). The Right to Be Forgotten in the Digital Age: The Challenges of Data Protection Beyond Borders. *German Law Journal*, *21*. https://doi.org/10.1017/glj.2020.14

Fadhillah, S. A., Matakupan, M. S. A., & Mingga, B. W. B. (2023). Peran Interpol dalam Penyelesaian Kasus Kejahatan Siber Berdasarkan Konvensi Budapest On Cybercrimes. *Journal on Education*, *5*(4). https://doi.org/10.31004/joe.v5i4.2822

Fitri, J. (2021). Pengaruh Internet Banking Dan Cyber Crime Terhadap Kepercayaan Nasabah Di Perbankan Syariah (Studi Pada Bank Syariah Mandiri Tapak Tuan). *Journal of Chemical Information and Modeling*, *53*(February).

Floridi, L. (2018). Soft ethics, the governance of the digital and the General Data Protection Regulation. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, *376*(2133). https://doi.org/10.1098/rsta.2018.0081

Goni, O. (2021). Cyber Crime and Its Classification. *International Journal of Electronics Engineering and Applications*, *10*(2). https://doi.org/10.30696/ijeea.x.i.2022.01-17

Goni, O., Md. Haidar Ali, Showrov, Md. Mahbub Alam, & Md. Abu Shameem. (2022). The Basic Concept of Cyber Crime. *Journal of Technology Innovations and Energy*, *1*(2). https://doi.org/10.56556/jtie.v1i2.113

Gundu, S. R., Charanarur, P., & Vijaylaxmi, J. (2025). Artificial Intelligence-Based Cybercrime Prevention and Data Security. In *Digital Defence: Harnessing the Power*

of Artificial Intelligence for Cybersecurity and Digital Forensics. https://doi.org/10.1201/9781032714813-9.

Hartono, B., Seregig, I. K., & Wibowo, B. (2021). Strategies in Countering Hoax and Hate Speech in Indonesia. *Sociological Jurisprudence Journal*, *4*(2). https://doi.org/10.22225/scj.4.2.2021.134-144

He, Z. (2022). When data protection norms meet digital health technology: China's regulatory approaches to health data protection. *Computer Law and Security Review*, *47*. https://doi.org/10.1016/j.clsr.2022.105758

Hapsari, R. D., & Pambayun, K. G. (2023). Ancaman Cybercrime Di Indonesia: Sebuah Tinjauan Pustaka Sistematis. *Jurnal Konstituen*, *5*(1), 1–17. https://doi.org/10.33701/jk.v5i1.3208

Hisbulloh, M. H. (2021). Urgensi Rancangan Undang-Undang (Ruu) Perlindungan Data Pribadi. *Jurnal Hukum Unissula*, *37*(2), 119–133. https://doi.org/10.26532/jh.v37i2.16272

Ivanyuk, V. (2024). Forecasting of digital financial crimes in Russia based on machine learning methods. *Journal of Computer Virology and Hacking Techniques*, *20*(3). https://doi.org/10.1007/s11416-023-00480-3

Indah, U., & Sari, P. (2021). Kebijakan Penegakan Hukum Dalam Upaya Penanganan Cyber Crime Yang Dilakukan Oleh Virtual Police Di Indonesia (Vol. 2).

Lubis, F. (2022). Cyber Crime E-Commerce Business Transactions. *SASI*, *28*(4). https://doi.org/10.47268/sasi.v28i4.1068

Maimon, D., & Louderback, E. R. (2019). Cyber-Dependent Crimes: An Interdisciplinary Review. In *Annual Review of Criminology* (Vol. 2). https://doi.org/10.1146/annurev-criminol-032317-092057

M Akbar Hadiprabowo, W. W. E. K. (2024). Pancasila in Modern Indonesian Legal Reform: Addresing Current Cases and International Debates on Ideology and Law. *Journal of Law and Legal Reform*, *4*(4), 2151–2174. https://doi.org/https://doi.org/10.15294/jllr.v5i4.18922.

Madung, O. G., & Stefanus, W. (2021). Constructing Modern Indonesia Based on Pancasila in Dialogue with the Political Concepts Underlying the Idea of Human Rights. *Journal of Southeast Asian Human Rights*, *5*, 1–24. https://doi.org/10.19184/jseahr

Muqsith, M. A., Muzykant, V. L., Tayibnapis, R. G., & Pratomo, R. R. (2022). Revolutionizing Pancasila as the ideology of Indonesians. *RUDN Journal of Sociology*, *22*(4), 860–871. https://doi.org/10.22363/2313-2272-2022-22-4-860-871.

Nunuk Sulisrudatin, Analisa Kasus Cybercrime Bidang Perbankan Berupa Modus

Pencurian Data Kartu Kredit, Jurnal Ilmiah Hukum Dirgantara, 2 Volume 9 No. 1, September 2018, https://journal.universitassuryadarma.ac.id/index.php/jihd/article/

Nayar, K., & Rathod, P. (2021). Cyber security challenges in indian banks. *Quarterly Bi-Lingual Research Journal*, *8*(29).

Nyoman Juwita Arsawati, I., Made Wirya Darma, I., & Antari, P. E. D. (2021). A criminological outlook of cyber crimes in sexual violence against children in Indonesian Laws. *International*

Prakoso, P. F. R. E. H. (2024). Pancasila as a Foundation for Legal Reform: Evaluating the Impact of Civic Education on Indonesian Legal Systems. *Journal of Law and Legal Reform*, *5*(3), 1429–1468. https://doi.org/https://doi.org/10.15294/jllr.v5i3.16498

Prof. Moeljatno, S. H. (2021). KUHP (Kitab Undang-Undang Hukum Pidana). *Bumi Aksara*.

Rao, T. K. R. K., Balagoni, Y., Vekariya, V., Irfan, B. M., Vasmatkar, A. D., Patil, H., Selvan, P., Natarajan, K., & Rajaram, A. (2024). Cybersecurity And Artificial Intelligence For Predicting Crime Rates. *Journal of Environmental Protection and Ecology*, *25*(5), 1395 – 1404. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85204039539&partnerID=40&md5=828def2054e9aeace386fda00fac92d3

Rian Dwi Hapsari, K. G. (2023). ANCAMAN CYBERCRIME DI INDONESIA . *Jurnal Konstituen*, Vol.5, 1-17. Rowe, N. C. (2019). Honeypot deception tactics. Autonomous Cyber Deception: Reasoning, Adaptive Planning, and Evaluation of HoneyThings, 35–45. https://www.researchgate.net/publication/330084850_Honeypot_Deception_Tactics_Reasoning_Adaptive_Planning_and_Evaluation_of_HoneyThings

Journal of Criminology and Sociology, *10*. https://doi.org/10.6000/1929-4409.2021.10.26

Romansky, R. P. (2022). Digital Age and Personal Data Protection. *International Journal on Information Technologies & Security, 14*(3).

Rosy, A. F. (2020). Kerjasama Internasional Indonesia: Memperkuat Keamanan Nasional di Bidang Keamanan Siber. *Journal of Government Science (GovSci) : Jurnal Ilmu Pemerintahan*, *1*(2). https://doi.org/10.54144/govsci.v1i2.12

Sari, U. I. (2021). Kebijakan Penegakan Hukum Dalam Upaya Penanganan Cyber Crime Yang Dilakukan Oleh Virtual Policedi Indonesia. *Mimbar Jurnal Hukum*, Volume 2 Nomor. 1 .

Sudarmadi, D. A., & Runturambi, A. J. S. (2019). Strategi Badan Siber dan Sandi Negara (BSSN) Dalam Menghadapi Ancaman Siber di Indonesia. *Jurnal Kajian Stratejik Ketahanan Nasional*, *2*(2), 7.

Sulisrudatin, N. (2018). *ANALISA KASUS CYBERCRIME BIDANG PERBANKAN BERUPA MODUS PENCURIAN DATA KARTU KREDIT* (Vol. 9, Issue 1). www.detikinet.com.

Santoso, R., & Adha, M. M. (2019). Inovasi Pendidikan Karakter melalui Pembelajaran Berbasis Lingkungan Sosial dan Budaya. *Prosiding Seminar Nasional Pendidikan FKIP Universitas Lampung*, 568–575.

Santoso, R., & Wuryandani, W. (2020). Pengembangan Bahan Ajar PPKn Berbasis Kearifan

Lokal Guna Meningkatkan Ketahanan Budaya Melalui Pemahaman Konsep Keberagaman. *Jurnal Ketahanan Nasional*, *26*(2), 229. https://doi.org/10.22146/jkn.56926

Silalahi, P. H., Dameria, F. A., & Dameria, F. A. (2023). Perlindungan Data Pribadi Mengenai Kebocoran Data Dalam Lingkup Cyber Crime Sebagai Kejahatan Transnasional. *Wajah Hukum*, *7*(2). https://doi.org/10.33087/wjh.v7i2.1244

Suharto, M. A., & Maria Novita Apriyani. (2021). Konsep Cyber Attack, Cyber Crime, Dan Cyber Warfare Dalam Aspek Hukum Internasional. *Risalah Hukum*. https://doi.org/10.30872/risalah.v17i2.705

Timofeyev, Y., & Dremova, O. (2022). Insurers' responses to cyber crime: Evidence from Russia. *International Journal of Law, Crime and Justice*, *68*. https://doi.org/10.1016/j.ijlcj.2021.100520

Yuspin, W., Wardiono, K., Nurrahman, A., & Budiono, A. (2023). Personal Data Protection Law in Digital Banking Governance in Indonesia. *Studia Iuridica Lublinensia*, *32*(1). https://doi.org/10.17951/sil.2023.32.1.99-130Sari, M. A. (2020). *Penelitian Kepustakaan (Library Research) dalam Penelitian Pendidikan IPA*.