ULR
UIN LAW REVIEW: JOURNAL LAW AND HUMAN RIGHTS
FAKULTAS SYARIAH DAN HUKUM
UIN SYARIF HIDAYATULLAH JAKARTA

PEMBENTUKAN *CYBER SECURITY* SEBAGAI UPAYA PERLINDUNGAN HUKUM MELALUI E-COMMERCE BERDASARKAN *DETERRENCE THEORY*

ESTABLISHMENT OF CYBER SECURITY AS A MEANS OF LEGAL PROTECTION THROUGH E-COMMERCE BASED ON DETERRENCE THEORY

Rika Rahayu1*, Chairil Qisthy Abidy, Anis Sepri Yadika Sinaga, dan Muhammad Reivan Aryasatya

[1]*UIN Syarif Hidayatullah Jakarta*
*Korespondensi: rrika8168@gmail.com

ARTICLE INFO

Vol. 2, No. 1 (2026): UIN Law Review
Hal. 74-55
E-ISSN: 3124-4459
DOI
Diajukan: 20-05-2026
Ditelaah: 28-05-2026
Direvisi: 05-06-2026
Diterima: 11-06-2026

Key Words: *Cyber Crime; Cyber Security; Deterrence Theory; E-Commerce; Law Protection.*

Kata Kunci: *Cyber Crime; Cyber Security; Deterrence Theory;* Perlindungan Hukum.

ABSTRACT

The implementation of Society 5.0 encourages the transformation of digital transactions through e-commerce, opening up strategic opportunities for MSMEs. However, this disruption also increases the risk of cyber crime due to weak legal protection. Therefore, a regulatory strategy based on juridical analysis is needed to form a comprehensive cybersecurity system. This research aims to formulate ideal regulations to improve legal protection against cyber crime in e-commerce and create a deterrent effect for criminals. Through a normative juridical approach, this study proposes the establishment of a Cybersecurity Institute to create a secure e-commerce sector.

ABSTRAK

Implementasi Society 5.0 mendorong transformasi transaksi digital melalui e-commerce, membuka peluang strategis bagi UMKM. Namun, disrupsi ini juga meningkatkan risiko cyber crime akibat lemahnya perlindungan hukum. Oleh karena itu, diperlukan strategi regulatif berbasis analisis yuridis untuk membentuk sistem keamanan siber yang komprehensif. Penelitian ini bertujuan merumuskan regulasi ideal untuk meningkatkan perlindungan hukum terhadap cyber crime pada e-commerce dan menciptakan efek jera bagi pelaku kejahatan. Melalui pendekatan yuridis normatif, penelitian ini mengusulkan pembentukan Lembaga Keamanan Siber untuk menciptakan sektor e-commerce yang aman.

1. PENDAHULUAN

Kemunculan *Society* 5.0 meningkatkan sistem perdagangan elektronik seperti *e-commerce* dan pembayaran digital sehingga mengubah cara masyarakat dalam melakukan kegiatan ekonomi yang lebih mudah. Transformasi transaksi 5.0 mengenalkan konsep *cashless society* melalui kegiatan perdagangan digital yang memungkinkan seluruh transaksi finansial masyarakat dilakukan secara non-tunai [1]. Perkembangan teknologi digital yang pesat telah menciptakan budaya masyarakat baru yang melibatkan pihak Usaha Mikro Kecil dan Menengah (UMKM) dalam dunia perdagangan digital. Selain menciptakan peluang terhadap pelaku usaha dan konsumen dalam kemudahan bertransaksi, perkembangan ini juga memiliki tantangan seperti tingginya kasus *cyber crime* pada platform *E-commerce* dikarenakan *cyber security* yang lemah. Ironisnya, pesatnya perkembangan teknologi tersebut belum diakomodir oleh hukum yang memadai. Alhasil, hukum kembali tertinggal oleh fenomena masyarakat karena ketiadaan perlindungan *cyber crime* pada *e-commerce*.

Mengacu pada data dari Kementerian Koperasi dan UKM pada tahun 2023, sektor UMKM menyumbang 61% terhadap Produk Domestik Bruto (PDB) Indonesia, sekaligus menyerap 97% dari total tenaga kerja. Adanya digitalisasi *e-commerce* ini, UMKM dapat memperluas pasar dan meningkatkan efisiensi bisnis sehingga menyumbang lebih banyak pada pembangunan ekonomi di Indonesia. Buktinya, Kementerian Koperasi dan UKM menemukan sebanyak 25,5 juta UMKM telah bertransformasi dan masuk ke dalam ekosistem digital per juli 2024 [2]. Mirisnya banyak UMKM yang tergabung dalam *e-commerce* harus menghadapi tantangan baru berupa ancaman kejahatan siber sebesar 61% atau senilai dengan Rp9.580 triliun [3]. Salah satu dampak cyber crime berupa kasus kebocoran data Tokopedia pada tahun 2022, di mana sebanyak 91 juta akun konsumen dan 7 juta akun merchant mengalami peretasan [4]. Selain itu pada Maret 2019, Bukalapak mengalami percobaan peretasan yang mengakibatkan kebocoran sebanyak 13 juta data

[1] Hermaya Ompusunggu dan Poniman Poniman, "Studi Empiris Sistem Pembayaran Cashless Dan Cardless," *Owner* 8, no. 2 (2024): 1117–24, https://doi.org/https://doi.org/10.33395/owner.v8i2.2037.

[2] Shofi Ayudiana, "Kemenkop UKM: 25,5 Juta UMKM Telah 'Go Digital,'" www.antara.com, 2024, https://www.antaranews.com/berita/4397157/kemenkop-ukm-255-juta-umkm-telah-go-digital.

[3] Kementerian Koordinator Bidang Perekonomian Republik Indonesia, "Dorong UMKM Naik Kelas Dan Go Export, Pemerintah Siapkan Ekosistem Pembiayaan Yang Terintegras," 2023, https://www.ekon.go.id/publikasi/detail/5318/dorong-umkm-naik-kelas-dan-go-export-pemerintah-siapkan-ekosistem-pembiayaan-yang-terintegrasi.

[4] C N N Indonesia, "Kronologi Lengkap 91 Juta Akun Tokopedia Bocor Dan Dijual," www.cnnindonesia.com, 2020, https://www.cnnindonesia.com/teknologi/20200503153210-185-499553/kronologi-lengkap-91-juta-akun-tokopedia-bocor-dan-dijual.

pengguna. Fakta kasus ini menjadi bukti nyata lemahnya perlindungan siber dalam sektor *e-commerce* di Indonesia.

Kasus kebocoran data di atas dapat merusak kepercayaan konsumen dan berdampak negatif pada reputasi bisnis, kepercayaan masyarakat terhadap keamanan transaksi digital, serta kerugian finansial bagi UMKM itu sendiri [5]. Mestinya negara menjamin keamanan bertransaksi termasuk data pribadi dan mendapatkan penghidupan yang layak melalui UMKM sebagaimana tercantum dalam amanat konstitusi Pasal 28D Ayat (1) dan Pasal 27 Ayat (1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 (UUD NRI 1945). Ironisnya, Regulasi *e-commerce* yang diimplementasikan di Indonesia masih ditemukan celah hukum dalam melindungi UMKM dari *cyber crime*. Pada pasal 65 Undang-Undang Nomor 7 Tahun 2014 tentang Perdagangan (UU Perdagangan) mengatur bahwa pelaku usaha dalam *e-commerce* wajib memberikan informasi dan data dengan akurat serta harus menjaga keamanan dalam bertransaksi secara elektronik. Namun, pada pasal ini tidak secara tegas mendefinisikan standar keamanan seperti apa yang harus diterapkan oleh platform *e-commerce*. Meskipun standar keamanan telah tercantum secara implisit dalam Pasal 61 Ayat (2) Peraturan Pemerintah Nomor 80 Tahun 2019 tentang Perdagangan Melalui Sistem Elektronik (PP PMSE) yang ditentukan oleh BSSN, Gubernur BI dan Ketua OJK. Hanya saja hingga saat ini, dalam Pasal 19 Peraturan Presiden Nomor 28 Tahun 2021 tentang Badan Siber dan Sandi Negara (Perpres BSSN) tidak ditemukan lembaga khusus keamanan siber di bidang e-commerce maupun ekonomi digital dalam ranah deputi keamanan siber dan sandi di bidang perekonomian.

Keamanan siber dalam bertransaksi di e-commerce termasuk pada hak dasar konsumen yang tercantum dalam Pasal 4 Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen (UU Perlindungan Konsumen). Konsumen *e-commerce* yang sejatinya terdiri dari pelaku usaha dan pembeli seharusnya dapat bertransaksi dengan aman melalui perlindungan dan lembaga khusus yang kompeten. Oleh karenanya, ketiadaan pengaturan mengenai keamanan siber di bidang *e-commerce* serta nihilnya lembaga pengawas khusus siber di Indonesia menyebabkan permasalahan ekonomi dan teknologi menjadi urgen untuk ditindaklanjuti.

Berdasarkan analisis terhadap regulasi di atas, terlihat jelas bahwa terdapat celah hukum yang membuat UMKM dan konsumen rentan terhadap kejahatan siber dalam sistem *e-commerce*. Tidak adanya standar keamanan siber yang jelas membuat UMKM menghadapi berbagai modus penipuan online, phishing, hingga kebocoran data yang bisa berujung pada kerugian besar. Maka dari itu, perlu adanya penelitian lebih lanjut untuk menemukan solusi berupa pembentukan lembaga pengawasan khusus siber di sektor perdagangan agar kegiatan transaksi dapat menjadi ruang

[5] CNN Indonesia, "13 Juta Data Bocor Bukalapak Dijual Di Forum Hacker," www.cnnindonesia.com, 2020, https://www.cnnindonesia.com/teknologi/20200506065657-185-500477/13-juta-data-bocor-bukalapak-dijual-di-forum-hacker.

aman bagi seluruh elemen masyarakat melalui artikel penelitian ini, yang berjudul "Pembentukan *Cyber Security* sebagai Upaya Perlindungan Hukum Melalui *E-commerce* Berdasarkan *Deterrence Theory*"Penulis merumuskan dua permasalahan yaitu: Pertama, Bagaimana problematika perlindungan hukum terhadap *cyber crime* dalam transaksi melalui *e-commerce*? Kedua, Bagaimana pengawasan ideal terhadap *e-commerce* melalui *cyber security* sebagai bentuk perlindungan siber di Indonesia?

2. METODE PENELITIAN

Karya Tulis Ilmiah ini menggunakan jenis penelitian yuridis normatif, yakni metode pengkajian hukum sebagai kaidah atau norma yang berlaku sehingga menjadi acuan setiap orang. Menurut Peter Mahmud Marzuki, penelitian yuridis normatif merupakan suatu proses untuk menemukan suatu aturan hukum, prinsip-prinsip hukum, maupun doktrin hukum guna menjawab permasalahan hukum yang dihadapi [6]. Adapun pendekatan penelitian yang digunakan yaitu pendekatan peraturan perundang-undangan (*statute approach*), pendekatan konseptual (*conceptual approach*), dan pendekatan komparatif (*comparative approach*).

Pada pendekatan peraturan perundang-undangan (*statute approach*) dimaksudkan untuk menelaah seluruh regulasi yang terkait dengan *cyber protection* dalam transaksi *e-commerce* terhadap pelaku UMKM. Adapun pendekatan konseptual dimaksudkan untuk menganalisis makna dalam suatu peraturan perundang-undangan melalui norma, nilai-nilai, serta latar belakang yang terkandung di dalamnya. Hal ini, pendekatan konseptual (*conceptual approach*) digunakan untuk menelaah regulasi dalam mengawasi pelaku UMKM terhadap *cyber crime* berbasis transaksi digital. Selain itu, pendekatan komparatif digunakan dalam pencarian gagasan dan solusi hukum pembentukan regulasi badan perlindungan *cyber crime* yang mengacu pada negara Amerika Serikat.

Bahan hukum berfungsi sebagai sumber penelitian hukum guna memecahkan suatu permasalahan hukum yang dihadapi. Hal ini, bahan hukum yang digunakan peneliti dalam melakukan penelitian hukum yuridis normatif ini berdasarkan pada bahan hukum primer, sekunder, dan tersier.

- Bahan Hukum Primer

Peter Mahmud Marzuki berpendapat bahwa, bahan hukum primer yaitu bahan hukum yang berwenang atau memiliki kekuasaan, meliputi peraturan perundang-undangan, catatan-catatan resmi atau risalah dalam pembuatan perundang-undangan maupun putusan hakim [7]. Bahan hukum primer dalam penelitian ini mencangkup:

- Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen
- Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik
- Undang-Undang Nomor 7 Tahun 2014 tentang Perdagangan

[6] Peter Mahmud Marzuki, *Penelitian Hukum* (Jakarta: Kencana Prenada Group, 2007).
[7] Marzuki.

- Peraturan Pemerintah Nomor 80 Tahun 2019 tentang Perdagangan Melalui Sistem Elektronik.
- Peraturan Presiden Nomor 28 Tahun 2021 tentang Badan Siber dan Sandi Negara.
- Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

- Bahan Hukum Sekunder

Peter Mahmud Marzuki, berpendapat bahwa bahan hukum sekunder merupakan semua laporan yang bukan merupakan dokumen resmi, meliputi buku teks, kamus hukum, jurnal hukum, dan komentar atas putusan pengadilan [8]. Bahan hukum sekunder dalam penelitian ini adalah buku-buku hukum, jurnal hukum, dan bahan internet yang berkaitan dengan penelitian ini.

- Bahan Hukum Tersier

Bahan hukum tersier merupakan pendukung dan pelengkap dari bahan hukum primer dan bahan hukum sekunder. Bahan hukum tersier dalam penelitian ini berupa kamus hukum ataupun ensiklopedia hukum yang berkaitan *dengan cyber protection* dan perlindungan UMKM terhadap *e-commerce*.

Teknik analisis data pada jenis penelitian yuridis normatif menggunakan teknik kepustakaan atau library research. Library research yaitu menggunakan dokumen sebagai bahan penelitiannya. Teknik library research dapat bersumber dari perpustakaan, artikel jurnal, dan media internet. Metode analisis data yang digunakan pada penelitian ini adalah metode deskriptif-analisis dan metode preskriptif. Metode deskriptif-analisis digunakan untuk menganalisis secara mendetail mengenai pokok-pokok permasalahan sehingga nantinya mampu mendapatkan solusi yang tepat untuk mengatasinya [9]. Sedangkan metode perskriptif digunakan untuk menganalisis mengenai regulasi yang seharusnya dilakukan untuk menyelesaikan permasalahan.

Teknik pengolahan data pada penelitian ini menggunakan beberapa langkah-langkah; pertama, identifikasi sumber bahan hukum maupun data; kedua, penyelesaian data sekunder serta penyusunan data yang berkaitan antara data primer dengan sekunder secara sistematis; ketiga, pencatatan serta kodifikasi sumber data yang diperlukan selama proses penulisan; keempat, klasifikasi data berdasarkan urutan perolehan; kelima, pengolahan data dalam bentuk uraian yang mudah dipahami; keenam, menganalisis data-data tersebut dengan mengacu pada permasalahan penelitian serta dituangkan dalam bentuk kalimat yang jelas dan terstruktur.

Kesimpulan ialah hasil akhir berdasarkan uraian analisis dan pembahasan hasil hipotesis yang didukung oleh data dan bahan hukum. Penarikan kesimpulan ini menggunakan pendekatan deduktif, di mana pernyataan bersifat umum diambil

[8] Marzuki.

[9] Dr Siti Padjarajani, *Metodologi Penelitian Pendekatan Muldisipliner* (Gorontalo: Ideals Publishing, 2020).

dari pernyataan yang bersifat khusus berdasarkan logika yang dapat diterima [10]. Terakhir, saran sebagai masukan praktikal sehingga kedepannya dapat diimplementasikan menjadi penyelesaian atas permasalahan dalam penelitian ini.

3. HASIL DAN PEMBAHASAN

3.1. Problematika Perlindungan Hukum Terhadap Cyber Crime Dalam Transaksi Melalui E-Commerce

Kemajuan teknologi berbasis digital salah satunya mencangkup perdagangan online, sehingga secara otomatis perdagangan digital akan berubah untuk menyediakan berbagai hal yang dibutuhkan masyarakat, salah satunya ialah pasar digital atau e-commerce. Namun, di balik kemajuan ini, terdapat tantangan besar terkait perlindungan hak konsumen. Fokus Keamanan transaksi, perlindungan konsumen, serta kemitraan dengan UMKM menjadi prioritas utama dalam menghadapi perubahan dinamika pasar. Perkembangan ini menunjukkan bagaimana e-commerce beradaptasi dengan permintaan pasar yang semakin meningkat, seiring dengan meningkatnya jumlah konsumen dan pencakupan digital di seluruh negara [11]. Tantangan besar dalam perdagangan digital melalui praktik perdagangan digital masih marak terjadi dan berpotensi merugikan konsumen, seperti penyalahgunaan data pribadi, penipuan transaksi, maupun kurangnya transparansi dalam mekanisme pengembalian barang.

Pada era digital, perlindungan konsumen menjadi semakin penting sehingga hukum berperan sebagai alat yang terus berkembang untuk menjaga hak-hak setiap orang. Aksioma tersebut sejalan dengan pendapat Satjipto Rahardjo terkait dengan perlindungan hukum, bahwa perlindungan hukum dilakukan ketika seseorang diberikan kekuasaan oleh hukum guna melindungi kepentingannya tersebut [12]. Sebagai otoritas yang memiliki kekuasaan, negara wajib memberikan perlindungan hukum bagi konsumen melalui pengendalian atas data pribadi mereka termasuk hak untuk mengetahui, mengelola, serta melindungi informasi pribadi dari penyalahgunaan data. Hak ini bukan sekadar aturan formalitas, tetapi bagian dari pemenuhan HAM yang secara fundamental menyangkut privasi dan keamanan individu dalam ruang digital. Apabila hukum gagal mengalokasikan kekuasaan ini secara efektif, konsumen menjadi rentan terhadap eksploitasi data, pencurian identitas, atau bahkan kejahatan siber yang lebih kompleks.

Urgensi regulasi yang ketat dalam permasalahan ini juga harus diimbangi dengan peran perusahaan e-commerce dalam menjaga hak konsumen yang menjadi perhatian utama. Platform digital diharapkan mampu menerapkan kebijakan transparansi, keamanan transaksi, serta meningkatkan kualitas layanan pelanggan.

[10] J M Muslimin, *Logika Dan Penalaran Hukum* (Tangerang Selatan: Pustaka Pedia, 2021).

[11] Yuyut Prayuti, "Dinamika Perlindungan Hukum Konsumen Di Era Digital: Analisis Hukum Terhadap Praktik E-Commerce Dan Perlindungan Data Konsumen Di Indonesia," *Jurnal Interpretasi Hukum* 5, no. 1 (2024): 903–13, https://doi.org/10.22225/juinhum.5.1.8482.903-913.

[12] Sutjipto Rahardjo, *Ilmu Hukum* (Bandung: Alumni, 1982).

Perusahaan yang menerapkan standar perlindungan konsumen yang tinggi cenderung mendapatkan kepercayaan lebih dari pelanggan, yang pada akhirnya berdampak positif terhadap keberlanjutan bisnis mereka [13]. Karenanya, sinergi antara pemerintah, pelaku bisnis, serta konsumen sangat diperlukan sebagai upaya perlindungan hak-hak konsumen, sehingga mewujudkan sektor digital yang setara bagi pihak terkait.

Perkembangan perdagangan elektronik di ASEAN yang begitu pesat, menyebabkan perlunya regulasi yang kuat dan mampu menjamin hak bagi konsumen. ASEAN Agreement on Electronic Commerce menetapkan bahwa negara anggota harus memastikan konsumen memiliki akses terhadap informasi yang jelas dan tidak menyesatkan dalam transaksi digital [14]. Upaya meningkatkan perlindungan konsumen dalam transaksi digital, OECD Guidelines on Consumer Protection in E-Commerce memiliki peran krusial dalam memastikan keamanan konsumen dan perdagangan digital serta mengharuskan perusahaan untuk menyediakan informasi yang jelas [15]. OECD mendorong pengembangan platform pengaduan online serta alternatif penyelesaian sengketa yang dapat diakses oleh konsumen lintas negara. Konvensi tersebut menyediakan mekanisme pengaduan yang efektif bagi konsumen serta memastikan pelaku usaha menjalankan bisnisnya secara etis dan bertanggung jawab.

Sejalan dengan itu, United Nations Guidelines for Consumer Protection mengharuskan perusahaan agar menyediakan informasi yang transparan tentang produk dan layanan yang ditawarkan, termasuk risiko yang mungkin timbul serta memastikan bahwa kontrak digital tidak mengandung klausul yang merugikan konsumen dalam mengajukan komplain [16]. Negara-negara dianjurkan untuk mengembangkan program literasi digital, juga mendorong negara-negara untuk bekerja sama dalam penegakan hukum perlindungan konsumen lintas batas, sehingga konsumen tetap mendapat perlindungan meskipun bertransaksi dengan pelaku usaha dari negara lain.

Indonesia telah mengatur perlindungan konsumen pada platform e-commerce dengan munculnya layanan seperti PrivyID yang memuat tanda tangan digital dan verifikasi identitas untuk memastikan transaksi online yang aman dan terpercaya [17]. Namun sayangnya, hal ini juga membawa tantangan baru terutama dalam sektor

[13] Muhammad Naufal Farras and Harits Ar Rosyid, "Perdagangan Elektronik Pada Industri 4.0 Dan Society 5.0," *Jurnal Inovasi Teknologi Dan Edukasi Teknik* 3, no. 3 (2023): 122–27, https://doi.org/10.17977/um068v3i32023p122-127.

[14] A.S.E.A.N., "ASEAN Agreement on Electronic Commerce," 2019, https://agreement.asean.org/media/download/20190306035048.pdf.

[15] "OECD Recommendation of the Council on Consumer Protection in E-Commerce," in *OECD Recommendation of the Council on Consumer Protection in E-Commerce*, 2016, https://doi.org/10.1787/9789264255258-en.

[16] Robert N Mayer, "United Nations Guidelines for Consumer Protection," *Watchdogs and Whistleblowers: A Reference Guide to Consumer Activism*, 2015, 489–92.

[17] Privy, "Efisiensi Dan Pengguna Data Pengguna: 2 Hal Yang Harus Diperhatikan Di Era Revolusi Industri 4.0," privy.id, 2018, https://privy.id/blog/2-revolusi-industri-4/.

keamanan khususnya perlindungan data pribadi. Oleh karena itu, layanan PrivyID harus lebih memanfaatkan teknologi canggih guna membantu meningkatkan transparansi serta memperkuat keamanan dalam setiap transaksi digital.

Lebih lanjut, negara Indonesia telah memberikan dasar bagi perlindungan hak-hak konsumen yang dicantumkan dalam konstitusinya. Pasal 28G ayat (1) UUD 1945 menyatakan bahwa setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang berada di bawah kekuasaannya [18]. Dalam konteks perdagangan digital, ini mencakup perlindungan data pribadi dan keamanan transaksi daring. Selain itu, Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen juga menegaskan bahwa konsumen berhak mendapatkan informasi yang benar, keamanan dalam transaksi, serta perlindungan dari praktik yang merugikan [19]. Namun, dengan pesatnya perkembangan e-commerce dan meningkatnya ancaman siber, diperlukan revisi atau regulasi tambahan yang lebih spesifik dalam menangani perlindungan hukum di ranah digital. Ancaman siber dalam perdagangan digital semakin kompleks, termasuk phishing, data breach, hingga penipuan transaksi. Oleh karena itu, penguatan regulasi di sektor ini menjadi krusial agar hak-hak konsumen dapat terjaga dengan baik.

Perdagangan digital mencangkup struktur regulasi yang telah berkembang diberbagai wilayah hukum, terutama mengenai perlindungan konsumen dan data menjadi aspek krusial dalam sektor e-commerce, mengingat mayoritas transaksi diselenggarakan melalui media digital seperti situs web dan aplikasi khusus. Proses verifikasi identitas pelanggan berfungsi sebagai mekanisme utama dalam mencegah tindak kejahatan siber dan aktivitas ilegal lainnya. Regulasi terkait privasi data diberlakukan dengan pengawasan ketat, sebagaimana diatur dalam GDPR di Uni Eropa dan Undang-Undang Perlindungan Data Pribadi di berbagai negara. Ancaman siber yang paling signifikan mencakup serangan malware dan ransomware, yang mampu mengganggu operasional sistem serta mengikis kepercayaan pengguna terhadap layanan [20].

Sejalan dengan Prof. Dr. Rhenald Kasali yang berpendapat bahwa perdagangan digital telah mengubah landscape bisnis secara dramatis, mendorong perusahaan untuk beradaptasi dengan cepat atau tertinggal [21]. Namun, transformasi ini harus diimbangi dengan regulasi yang melindungi konsumen dan memastikan persaingan dengan sehat. Maka dari itu, penting untuk pemerintah segera merumuskan regulasi yang lebih baik dalam perdagangan digital. Regulasi ini harus mampu melindungi

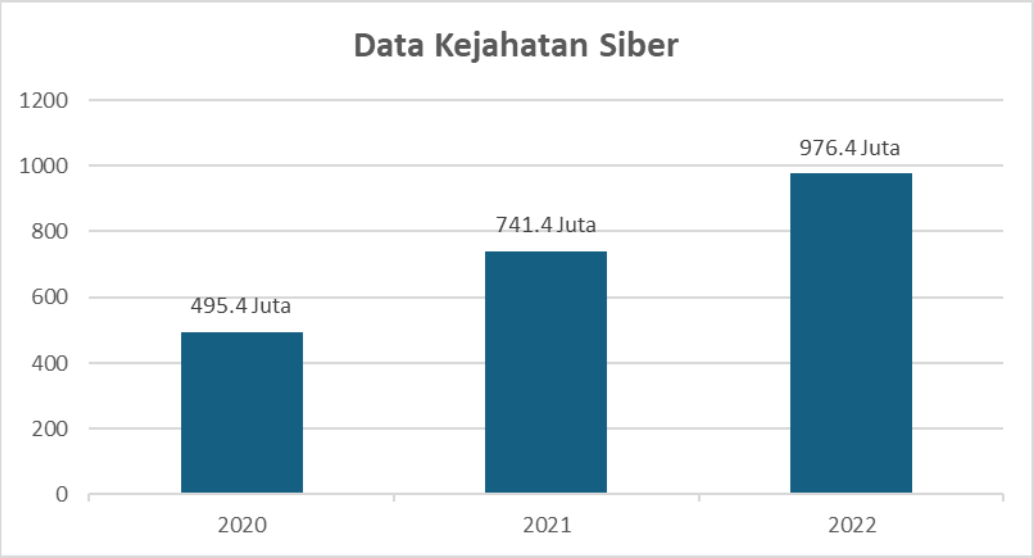
[18] Indonesia, "Undang-Undang Dasar Negara Republik Indonesia Tahun 1945," 1945.

[19] Republik Indonesia, "Undang-Undang Nomor 8 Tahun 1999 Perlindungan Konsumen," n.d., https://peraturan.bpk.go.id/Home/Details/45288/uu-no-8-tahun-1999.

[20] Fani Ma'sumatul Maghfiroh, "Kolaborasi Salam Berbasis Crowdfunding," in *Proceedings of Islamic Economics, Business, and Philanthropy*, vol. 2, 2023.

[21] Rhenald Kasali, *Change!: Pemimpin Dan Organisasi Dalam Pusaran Disrupsi* (Jakarta: Jakarta, 2020).

konsumen, mendorong persaingan sehat, dan memastikan bahwa inovasi dapat terus berkembang.



Gambar 1.1 Grafik Peningkatan Data Cyber Crime

Tantangan dalam perdagangan digital tidak hanya sebatas regulasi, tetapi juga ancaman kejahatan siber yang semakin meningkat. Menurut laporan data trafik Badan Siber dan Sandi Negara (BSSN), menunjukkan peningkatan yang signifikan terkait dengan kejahatan siber di Indonesia dalam tiga tahun terakhir. Pada tahun 2020, tercatat Indonesia mengalami serangan siber mencapai angka 495,4 juta. Sementara, pada tahun 2021 kejahatan siber melonjak menjadi 741,4 juta atau meningkat 49% dari tahun sebelumnya. Meningkatnya kejahatan siber ini juga terjadi pada tahun 2022 yang mencapai angka 976,4 serta adanya peningkatan sebesar 31% dari tahun 2021 [22]. Makin meningkatnya kejahatan siber tersebut mencerminkan tingginya risiko keamanan di sektor digital, khususnya dalam sektor e-commerce atau perdagangan digital, sehingga hal ini perlu menekankan urgensi penguatan regulasi serta perlindungan kejahatan siber bagi pengguna dan pelaku usaha digital.

Meningkatnya ancaman kejahatan siber pada sektor perdagangan digital, menimbulkan dampak yang signifikan bagi beberapa pihak terutama konsumen dan pelaku usaha. Salah satu dampak utamanya adalah berkurangnya kepercayaan masyarakat terhadap transaksi digital akibat maraknya kasus kebocoran data pengguna, penipuan online, serta serangan peresetan yang merugikan konsumen [23]. Selain itu, UMKM juga mengalami serangan kejahatan siber berupa pencurian data

[22] Ratna Christianingrum, *Tantangan Penguatan Keamanan Siber Dalam Menjaga Stabilitas Keamanan* (Jakarta: Pusat Kajian Anggaran Keahlian DPR RI, 2021).

[23] Cindy Mutia Annur, "E-Commerce Indonesia Jadi Incaran, Peresetan Naik 6.000% Saat Pandemi," katadata.co.id, 2020, https://katadata.co.id/digital/e-commerce/5eeb755de99e5/e-commerce-indonesia-jadi-incaran-peretasan-naik-6000-saat-pandemi?utm_source.

pelanggan serta penipuan transaksi sehingga menyebabkan kerugian finansial besar bagi UMKM yang memiliki keterbatasan dalam keamanan siber.

Tingginya angka kejahatan siber dalam e-commerce sebagaimana data BSSN di atas menjadi salah satu ancaman krusial bagi pelaku UMKM maupun konsumen. Minimnya pengawasan khusus terhadap kejahatan siber dalam sektor perdagangan digital membuat para pelaku kejahatan siber semakin leluasa dalam bertindak. Adapun undang-undang yang mengatur perlindungan terhadap kejahatan siber dalam sektor perdagangan digital dinilai belum spesifik mengatur terkait hal tersebut. Misalnya, Undang-Undang Nomor 1 Tahun 2024 Tentang Perubahan Kedua Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (UU ITE) yang belum spesifik mengatur mekanisme pengawasan terhadap e-commerce [24]. UU ITE lebih berfokus pada aspek hukum terkait transaksi elektronik dan sanksi terhadap pelanggaran dalam sektor digital. Akibatnya, perlindungan bagi pelaku usaha dan konsumen pada transaksi digital yang belum optimal.

Selain UU ITE, regulasi lain yang berkaitan dengan perdagangan digital adalah UU Perdagangan. Meskipun UU ini mengatur terkait aspek perdagangan digital sebagaimana termaktub dalam Bab VIII, namun sayangnya regulasi tersebut belum dijelaskan secara eksplisit membahas perlindungan UMKM serta pengawasan kejahatan siber pada sektor e-commerce [25]. Ketentuan pidana pada Bab XVIII dalam UU Perdagangan khususnya pasal 115 hanya mengatur sanksi non-pidana bagi pelaku usaha yang melanggar tanpa adanya aturan spesifik terkait hukuman bagi platform e-commerce yang gagal melindungi transaksi digital [26].

Kekosongan regulasi dalam UU Perdagangan di atas terkait pengawasan kejahatan siber pada sektor e-commerce sebenarnya telah berusaha diatasi dengan Peraturan Pemerintah Nomor 80 Tahun 2019 Tentang Perdagangan Melalui Sistem Elektronik (PP PMSE) yang mengatur berbagai aspek perdagangan digital, termasuk kewajiban pelaku usaha dalam menjamin keamanan data konsumen serta mekanisme penyelesaian sengketa dalam transaksi digital. Namun sayangnya, PP PMSE belum mengatur mekanisme perlindungan hukum terhadap pelaku UMKM. Dibuktikan melalui Pasal 18 ayat (1) dan (3) mengatur bahwa konsumen yang mengalami kerugian dapat melaporkannya kepada Menteri, dan jika pelaku usaha tidak menyelesaikan masalah tersebut mereka akan masuk daftar pengawasan [27]. Akan tetapi, tidak ada ketentuan serupa bagi UMKM yang mengalami kerugian akibat platform e-commerce atau konsumen. Implikasinya, ketika UMKM

[24] Republik Indonesia, "Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik," n.d.

[25] Republik Indonesia, "Undang-Undang Republik Indonesia No. 7 Tahun 2014 Tentang Perdagangan," n.d., https://peraturan.bpk.go.id/Home/Details/38584/uu-no-7-tahun-2014.

[26] Republik Indonesia.

[27] Republik Indonesia, "Peraturan Pemerintah Republik Indonesia Nomor 80 Tahun 2019 Tentang Perdagangan Melalui Sistem Elektronik," n.d.

mengalami penipuan digital atau kebocoran data akibat platform e-commerce, tidak ada regulasi khusus yang melindungi mereka.

Meskipun PP PMSE mengatur perdagangan digital, aturan ini tidak secara spesifik menetapkan standar keamanan bagi platform e-commerce dalam melindungi transaksi digital. Akibatnya, UMKM rentan terhadap kebocoran data dan serangan siber, tanpa adanya regulasi yang mengharuskan platform e-commerce untuk memberikan kompensasi kepada UMKM apabila terjadi penipuan digital atau pencurian data. Pasal 22 PP PMSE hanya mengatur tanggung jawab PMSE terhadap konten informasi illegal, tanpa mencantumkan kewajiban atau sanksi bagi e-commerce yang gagal melindungi pelaku UMKM dari kejahatan siber, sehingga berpotensi membuat e-commerce lepas tanggung jawab jika terjadi kebocoran data atau transaksi digital yang merugikan UMKM [28]. Dampaknya, UMKM tidak memiliki kepastian hukum dalam menghadapi risiko kejahatan digital, sementara platform e-commerce tidak memiliki kewajiban yang jelas untuk melindungi UMKM dari ancaman tersebut.

Langkah strategis untuk mengatasi berbagai kelemahan regulasi guna melindungi pelaku usaha dari kejahatan siber dalam sektor e-commerce diperlukan pembaruan regulasi yang spesifik dan komprehensif. Selain itu, pembentukan lembaga pengawas khusus yang berfokus pada keamanan siber dalam sektor perdagangan digital juga menjadi solusi yang dapat meningkatkan perlindungan kepada UMKM maupun konsumen. Platform e-commerce juga diperlukan untuk meningkatkan standar keamanan data serta memberikan kompensasi bagi pelaku usaha yang mengalami kerugian akibat kelalaian sistem e-commerce. Adanya peraturan yang pasti dan sistem pengawasan yang intensif, sektor perdagangan digital dapat berjalan lebih aman serta berkelanjutan, sehingga meningkatkan kepercayaan masyarakat terhadap transaksi digital.

Data pribadi telah menjadi aset paling berharga baik individu maupun bagi organizations in the changing digital era. Dimana hal ini meliputi informasi yang dipakai guna mengidentifikasi data pribadi seseorang. Namun, bersamaan menggunakan peningkatan penggunaan teknologi informasi, resiko kebocoran data pribadi juga semakin tinggi. Kasus kebocoran data pribadi terjadi ketika informasi sensitif yang seharusnya terlindungi justru bocor atau dicuri oleh pihak yang tidak berwenang [29].

Salah satu contoh besar terjadi pada bulan Maret 2020, Tokopedia dilaporkan mengalami peretasan bahkan jumlahnya sebesar 91 juta akun, artinya hampir semua akun di Tokopedia berhasil dibobol oleh peretas. Pelaku kemudian menjual data yang berhasil diambil di dark web, yang mencakup ID pengguna, alamat email, nama lengkap, tanggal lahir, jenis kelamin, nomor ponsel, dan kata sandi yang masih terenskripsi. Komunitas Konsumen Indonesia (KKI) pun merespons kejadian ini

[28] Indonesia.

[29] Kaharudin and Zul Amirul Haq, *Kecerdasan Buatan Dan Aspek Perlindungan Hukum Di Era Digitalisasi* (Jakarta: Penada Kencana, 2024).

dengan mengajukan gugatan hukum atas kelalaian Menteri Komunikasi dan Informatika (Menkominfo) serta Tokopedia, sebab keduanya dinilai gagal melindungi data pribadi pengguna. Gugatan ini didaftarkan melalui sistem e-court di Pengadilan Negeri Jakarta Pusat pada 6 Mei 2020. Dalam tuntutannya, KKI meminta pengadilan untuk memerintahkan penghentian sementara sistem elektronik Tokopedia hingga ada putusan berkekuatan hukum tetap, serta menuntut agar Kominfo mencabut Tanda Daftar Penyelenggara Sistem Elektronik (PSE). Tokopedia juga diminta membayar denda administratif sebesar Rp100 miliar yang harus disetorkan ke kas negara dalam waktu maksimal 30 hari setelah putusan berkekuatan hukum tetap.

Selain itu pada Maret 2019, Bukalapak mengalami percobaan peretasan yang mengakibatkan kebocoran data sekitar 13 juta pengguna. Peretasan ini dilakukan oleh seorang hacker yang menggunakan nama samaran Gnostic Players, yang mengklaim telah mencuri data dari beberapa situs, termasuk Bukalapak. Data yang dicuri meliputi informasi pengguna dari tahun 2015 hingga 2017, dan hacker tersebut kemudian mencoba menjual data ini di dark web [30]. Bukalapak pada awalnya membantah bahwa data pribadi seseorang telah dicuri dalam peretasan tersebut. Mereka menyatakan bahwa upaya peretasan itu tidak berhasil merusak sistem keamanan mereka secara signifikan. Namun, setelah berita mengenai kebocoran ini muncul kembali pada Mei 2020, Bukalapak mengonfirmasi bahwa data yang dijual oleh hacker di forum adalah data yang dicuri pada Maret 2019, dan bukan merupakan kebocoran baru. CEO Bukalapak, Rachmat Kaimuddin, menegaskan bahwa mereka telah mengambil langkah-langkah untuk meningkatkan keamanan data pengguna dan memastikan bahwa tidak ada kebocoran baru setelah insiden tersebut [31].

Selain Tokopedia dan Bukalapak, platform e-commerce lainnya juga telah mengalami masalah serupa terkait kebocoran data, salah satunya adalah Bhinneka. com. Pada Mei 2020, Bhinneka.com mengalami kebocoran data yang mengakibatkan 1,2 juta data pengguna dijual secara bebas oleh kelompok peretas yang dikenal dengan nama ShinyHunter. Data pengguna Bhinneka.com dan 10 perusahaan serupa lainnya juga dijual di dark web, yang menyebabkan sekitar 73,2 juta data pribadi pengguna e-commerce dan data perusahaan lainnya terjual dengan harga mencapai USD 18 ribu per data [32]. Setelah insiden tersebut, Bhinneka.com melakukan investigasi bersama Kominfo untuk menilai keamanan sistem mereka

[30] KumparanTECH, "Bukalapak Akui 13 Juta Data Yang Dijual Hacker Adalah Peretasan Di Maret 2019," www.kumparan.com, 2019, https://kumparan.com/kumparantech/bukalapak-akui-13-juta-data-yang-dijual-hacker-adalah-peretasan-di-maret-2019-1tMRTr1UR0G.

[31] Faisal Hafis, "CEO Bukalapak Akui Kebocoran Data 13 Juta Akun Pengguna Tahun Lalu," Cyberheart.id, 2020, https://cyberthreat.id/read/6548/CEO-Bukalapak-Akui-Kebocoran-Data-13-Juta-Akun-Pengguna-Tahun-Lalu.

[32] C N N Indonesia, "Peretas Jual 1,2 Juta Data Pengguna Bhinneka.Com Di Dark Web," www.cnnindonesia.com, 2020, https://www.cnnindonesia.com/teknologi/20200511000424-185-501867/peretas-jual-12-juta-data-pengguna-bhinnekacom-di-dark-web.

dengan mengambil tindakan keamanan tambahan dan memberitahukan pengguna mengenai perlindungan data. [33]

Tindakan keamanan yang dilakukan oleh Bhinneka.com dengan menghimbau pengguna untuk mengganti kata sandi mereka sebagai tindakan pencegahan. Kasus ini menegaskan pentingnya bagi perusahaan e-commerce untuk memperkuat sistem keamanan siber guna mencegah terulangnya kejadian serupa di masa mendatang. Pengguna juga perlu lebih waspada dalam membagikan data pribadi mereka dan secara rutin memperbarui informasi keamanan akun. Perlu adanya regulasi yang lebih ketat serta sistem pengawasan yang lebih efektif agar insiden kebocoran data semacam ini tidak terulang dan terus merugikan masyarakat.

3.2 Pengawasan Ideal Terhadap E-commerce Melalui Cyber Security Sebagai Bentuk Perlindungan Siber Di Indonesia

Pesatnya perkembangan e-commerce membawa berbagai manfaat, tetapi juga menimbulkan hambatan terutama dalam hal perlindungan konsumen serta kepastian hukum, sehingga pengawasan berbasis aturan hukum menjadi krusial dalam menjaga keseimbangan inovasi teknologi serta perlindungan kepentingan publik. Pengawasan berbasis aturan hukum berdasarkan perspektif Rechtsstaat merupakan prinsip fundamental yang menjamin keadilan dengan menegakkan supremasi hukum dalam segala aspek kehidupan, termasuk dalam aktivitas ekonomi digital seperti e-commerce [34]. Negara berkewajiban untuk tidak hanya merancang, tetapi juga memastikan regulasi yang dapat menjamin keamanan menyeluruh terhadap konsumen baik dalam hal keamanan transaksi, perlindungan data pribadi, maupun jaminan terhadap hak-hak mereka sebagai pengguna layanan digital.

Pengawasan terhadap e-commerce harus dilakukan secara transparan dan dipertanggungjawabkan, dengan menerapkan mekanisme hukum yang jelas, sehingga penerapan prinsip Rechtsstaat dalam pengawasan e-commerce tidak hanya menciptakan sektor perdagangan digital yang aman dan adil, tetapi juga memastikan bahwa semua pihak, baik konsumen maupun pelaku usaha, tunduk pada hukum yang berlaku. Hal ini menunjukkan bahwa peran negara dalam mengawasi e-commerce tidak hanya sebatas menegakkan hukum, tetapi juga menjadi bagian dari upaya lebih luas dalam menciptakan keseimbangan antara kepentingan ekonomi dan perlindungan hak-hak masyarakat [35]. Oleh karena itu,

[33] Deanne Destriani Firmansyah Putri and Muhammad Helmi Fahrozi, "Upaya Pencegahan Kebocoran Data Konsumen Melalui Pengesahan Ruu Perlindungan Data Pribadi (Studi Kasus E-Commerce Bhinneka.Com," *Borneo Law Review* 5, no. 1 (2021): 46–68, https://doi.org/10.35334/bolrev.v5i1.2014.

[34] Rokilah Rokilah, "Dinamika Negara Hukum Indonesia: Antara Rechtsstaat Dan Rule Of Law," *Nurani Hukum* 2, no. 1 (2020): 12, https://doi.org/10.51825/nhk.v2i1.8167.

[35] I.Nyoman Putu Budiartha Anak Agung Made Ayu Rai Lidya Astari and Ni Made Puspasutari Ujianti, "Pengawasan Terhadap Transaksi Bisnis E-Commerce Dalam Mewujudkan

pengawasan oleh pemerintah terhadap pelaku usaha merupakan bentuk campur tangan dalam urusan kesejahteraan rakyatnya pada era digital.

Pengawasan ideal terhadap e-commerce melalui cyber security harus sejalan dengan prinsip perlindungan preventif dan represif. Implementasi perlindungan hukum preventif dilakukan dengan cara memberikan perlindungan hukum dalam hal pengawasan pada transaksi jual beli online melalui e-commerce guna mencegah terjadinya kejahatan siber yang tidak diinginkan. Perlindungan hukum preventif dapat diwujudkan melalui upaya pencegahan, seperti peningkatan kesadaran keamanan siber bagi pengguna, penerapan standar keamanan oleh penyedia layanan e-commerce, serta eksistensi regulasi yang mendukung kebijakan keamanan digital [36]. Sementara itu, perlindungan hukum represif sebagai upaya dalam penyelesaian suatu sengketa akibat adanya kasus yang merugikan pihak yang bersangkutan. Perlindungan hukum represif dapat diwujudkan melalui penerapan sanksi yang tegas terhadap pelanggaran keamanan siber. Pengawasan yang efektif juga memerlukan pendekatan kolaboratif, dimana pemerintah, penyedia layanan e-commerce, serta pengguna bekerja sama untuk menciptakan sektor digital yang aman dan terpercaya.

Perkembangan era digital membawa tantangan baru dalam HAM, khususnya terkait privasi dan keamanan digital, sehingga perlindungan data pribadi menjadi krusial seiring meningkatnya transaksi digital. Hal ini menuntut regulasi yang jelas untuk menjamin keseimbangan antara hak individu atas privasi dan kewajiban negara dalam menjaga keamanan siber yang diakui sebagai bagian dari HAM dalam berbagai instrumen hukum internasional. Oleh karena itu, keseimbangan antara perlindungan privasi dan keamanan digital dapat dicapai melalui penerapan kebijakan yang jelas, proporsional, dan berbasis HAM serta regulasi yang ada harus terus diperbarui dan disesuaikan dengan perkembangan teknologi agar dapat memberikan perlindungan yang optimal bagi masyarakat di era digital.

Transformasi ekonomi digital di Indonesia menjadi penggerak utama bagi roda perekonomian dalam beberapa tahun belakangan, didorong oleh peningkatan nilai ekonomi digital yang terus berkembang setiap tahunnya. Hal ini terbukti dengan tercatatnya nilai ekonomi digital Indonesia sebesar USD 44 Miliar pada tahun 2020, yang kemudian melonjak menjadi USD 63 Miliar pada tahun 2021 [37]. Tren perkembangan ekonomi digital ini terus berlanjut hingga tahun 2022 dengan

Perlindungan Konsumen," *Jurnal Konstruksi Hukum* 1, no. 1 (2020): 38–43, https://doi.org/10.22225/jkh.1.1.2126.38-43.

[36] Fandani Damayanti, "Hukum Perlindungan Konsumen Terhadap Barang Yang Tidak Sesuai Dengan Perjanjian E-Commerce," 2025.

[37] Candra Gunawan, "INFOGRAFIS:Nilai Ekonomi Digital Di Asia Tenggara, Indonesia Bakal Tumbuh Tiga Kali Lipat 2025," 2021, https://gokepri.com/infografis-nilai-ekonomi-digital-di-asia-tenggara-indonesia-bakal-tumbuh-tiga-kali-lipat-2025/.

capaian sebesar USD 77 Miliar serta tahun 2023 nilai ekonomi digital semakin meningkat menjadi USD 82 Miliar [38].

Seiring dengan tren positif yang terus berlanjut, prospek ke depan pun semakin optimis di mana ekspansi ekonomi digital diproyeksikan terus berkembang dengan perkiraan mencapai USD 90 Miliar pada tahun 2024 bahkan diperkirakan mencapai lebih dari USD 130 Miliar pada tahun 2025 [39]. Lonjakan ini mencerminkan semakin luasnya penerapan teknologi digital di berbagai sektor, mulai dari e-commerce, fintech, hingga layanan berbasis digital lainnya. Perkembangan ini tidak hanya membuka peluang baru bagi pelaku usaha, tetapi juga mempercepat inklusi ekonomi serta meningkatkan daya saing Indonesia di kancah global. Hal tersebut didukung dengan infrastruktur digital yang semakin kuat, kebijakan yang berpihak pada inovasi, serta meningkatnya kepercayaan masyarakat terhadap layanan digital, sehingga ekonomi digital di Indonesia diprediksi akan terus menjadi penggerak utama pertumbuhan ekonomi di tahun-tahun mendatang.

Jumlah pengguna e-commerce di Indonesia menunjukkan peningkatan yang penting pada beberapa tahun terakhir, hal ini telah didukung oleh data statistik yang dipublikasikan oleh Kementerian Perdagangan. Pada tahun 2020, jumlah pengguna e-commerce di Indonesia tercatat mencapai 38,7 juta. Tren pertumbuhan ini terus berlanjut dengan jumlah pengguna yang naik menjadi 44,4 juta pengguna pada 2021, kemudian meningkat lagi hingga 50,8 juta pengguna di tahun 2022.

Laju pertumbuhan yang kuat ini semakin terlihat pada 2023, di mana jumlah pengguna e-commerce melonjak menjadi 58,6 juta pengguna, menunjukkan peningkatan minat masyarakat terhadap transaksi digital. Proyeksi ke depan pun tetap optimis, dengan perhitungan bahwa pada tahun 2024 jumlah pengguna e-commerce akan menembus 65,6 juta [40]. Pertumbuhan ini didorong oleh berbagai faktor, termasuk meningkatnya penetrasi internet, kemudahan akses terhadap layanan digital, serta semakin banyaknya platform e-commerce yang menawarkan pengalaman belanja yang lebih praktis, aman, dan menarik bagi konsumen. Seiring dengan meningkatnya jumlah pengguna e-commerce, pelaku UMKM memiliki peluang lebih besar untuk mencakup market yang lebih luas serta mengembangkan daya saing mereka.

Prinsip-prinsip perlindungan konsumen dan penguatan regulasi di sektor e-commerce selaras dengan landasan konstitusional dalam pengelolaan perekonomian nasional tercermin dalam Pasal 33 Ayat (4) UUD NRI 1945 menegaskan bahwa perekonomian nasional harus berlandaskan pasa prinsip-

[38] Demis Rizky, "Masa Depan Ekonomi Indonesia Tak Secerah Dahulu Kala," www.cnbcindonesia.com, 2023, https://www.cnbcindonesia.com/tech/20231102074541-37-485689/masa-depan-ekonomi-digital-indonesia-tak-secerah-dahulu-kala.

[39] Komdigi, "Penggerak Inklusi Dan Pertumbuhan," komdigi.go.id, 2024, https://www.komdigi.go.id/berita/ekonomi-digital/detail/penggerak-inklusi-dan-pertumbuhan.

[40] PSDI Kementerian Perdagangan, "Perdagangan Digital (E-Commerce) Indonesia Periode 2023," 2024.

prinsip demokrasi ekonomi, yang mencakup asas kebersamaan, efisiensi berkeadilan berkelanjutan, kemandirian, serta stabilitas pertumbuhan dan integrasi sistem perekonomian negara [41]. Amanat konstitusi tersebut menjadi landasan bagi negara dalam menjamin bahwa implementasi kebijakan ekonomi tidak hanya berfokus pada perkembangan, tetapi juga menjaga kewenangan yang dijamin oleh konstitusi, pada konteks tersebut termasuk para pelaku UMKM pada sektor e-commerce. Sebagai bagian dari pengawasan hak-hak konstitusional, negara memiliki kewajiban untuk memastikan bahwa UMKM memperoleh perlindungan hukum yang memadai agar dapat bersaing secara adil di era digital. Pengawasan ini meliputi pengaturan terkait persaingan usaha yang sehat, perlindungan hak konsumen serta pelaku UMKM, dan pencegahan eksploitasi oleh platform e-commerce yang berpotensi merugikan UMKM.

Indonesia sebagai negara yang berlandaskan hukum memiliki kewajiban konstitusional untuk memastikan keadilan serta kepastian hukum bagi seluruh warganya termasuk para pelaku UMKM melalui tindakan seperti merevisi penambahan pasal pada PP PMSE guna memperjelas perlindungan hukum bagi UMKM dalam platform pasar digital termasuk penyediaan mekanisme pengaduan dan penyelesaian sengketa yang lebih efektif. Negara perlu meningkatkan pengawasan terhadap platform e-commerce agar tidak terjadi eksploitasi terhadap UMKM terutama dalam aspek persaingan usaha, perlindungan data, dan transparansi transaksi. Penetapan sanksi bagi e-commerce yang lalai melindungi pelaku UMKM juga menjadi langkah krusial, seperti pemberian denda administratif atau pembatasan operasional bagi e-commerce yang terbukti merugikan UMKM [42]. Pemerintah sebaiknya perlu membentuk lembaga atau unit khusus yang menangani perlindungan UMKM dalam transaksi digital, sehingga pelaku UMKM memiliki akses terhadap perlindungan hukum yang lebih mudah dan cepat.

Kehadiran negara sebagai pelindung akan memastikan bahwa perkembangan sektor digital tidak hanya menguntungkan perusahaan besar, tetapi juga memberdayakan usaha kecil agar dapat bersaing secara sehat. Kerja sama internasional menjadi salah satu pendekatan yang diambil oleh pemerintah Indonesia melalui kolaborasi dengan Australia dalam pengembangan keamanan siber. Kerja sama ini bertujuan untuk meningkatkan keterampilan tenaga ahli Indonesia dalam menghadapi ancaman siber global serta memperkuat kebijakan keamanan digital nasional [43]. Langkah ini sejalan dengan visi pemerintah guna mewujudkan lingkungan digital yang kondusif bagi industri dan sektor publik.

[41] Republik Indonesia, "Majelis Permusyawaratan Rakyat, UUD Negara RI Tahun 1945.," n.d.

[42] Muhammad Arbani, "Aspek Hukum Perlindungan Umkm Dalam Penjualan Di E-Commerce : Tantangan Dan Solusi Di Era Digital" 6, no. 2 (2025): 1166–75.

[43] Kementerian Koordinator Bidang Perekonomian RI, "Perkuat Sektor Keamanan Siber, Indonesia Dan Australia Jalin Kerja Sama Pengembangan SDM," 2025, https://www.ekon.go.id/publikasi/detail/6186/perkuat-sektor-keamanan-siber-indonesia-dan-australia-jalin-kerja-sama-pengembangan-sdm.

Selain penguatan SDM, strategi lain yang dikembangkan adalah peningkatan regulasi dan infrastruktur keamanan siber.

Urgensi pengawasan dalam sektor e-commerce di berbagai negara semakin meningkat seiring dengan pesatnya pertumbuhan transaksi daring. Lebih lanjut, dalam menghadapi tantangan transaksi digital Amerika Serikat memiliki lembaga perlindungan konsumen dalam e-commerce melalui Federal Trade Commision Act (FTC Act) dan Consumer Product Safety Act (CPSA). FTC diberi wewenang untuk menangani tindakan melawan hukum yang dilakukan oleh pelaku usaha sehingga konsumen merasa dirugikan. CPSA turut memperkuat perlindungan konsumen dengan menetapkan standar keselamatan produk dan memberi wewenang kepada Consumer Product Safety Commission (CPSC) guna melarang peredaran produk yang berpotensi membahayakan. Hal ini menggambarkan bahwa regulasi di Amerika Serikat lebih terkoordinasi dan tegas dalam menangani pelanggaran serta menjaga keamanan konsumen, sementara Indonesia menerapkan sistem civil law, sedangkan Amerika Serikat menggunakan sistem common law [44]. Sehingga, Indonesia harus memperkuat perlindungan hukum e-commerce, khususnya terkait pengawasan dan edukasi konsumen.

Tanpa pengawasan yang ketat, perkembangan e-commerce bisa berjalan tanpa arah yang jelas sehingga dibutuhkan regulasi yang mampu menyesuaikan perubahan yang terjadi. Perkembangan pesat teknologi digital dalam e-commerce menuntut adanya regulasi yang dapat mengakomodasi perubahan tersebut secara efektif. PP PMSE menjadi salah satu regulasi utama yang mengatur perdagangan digital, namun masih memiliki keterbatasan dalam mengadaptasi perkembangan teknologi baru seperti Artificial Intelligence (AI), big data, dan blockchain. UU ITE sebagai dasar hukum transaksi elektronik juga belum memberikan ketentuan yang secara eksplisit mengatur perlindungan konsumen dalam ekosistem digital yang terus berkembang.

Mekanisme ini menjadi langkah dan solusi baru dalam mewujudkan optimalisasi lembaga perlindungan cyber crime di Indonesia pada e-commerce dengan dibentuknya Lembaga Keamanan Siber Melalui Perdagangan Elektronik (LKSMPE). Lembaga ini merupakan hasil kolaborasi antara Badan Siber dan Sandi Negara (BSSN) melalui Deputi Bidang Keamanan Siber dan Sandi Negara, Kementerian Perdagangan yang diwakilkan oleh Direktorat Perdagangan melalui Sistem Elektronik dan Jasa, serta Otoritas Jasa Keungan (OJK) yang memiliki fokus utama sebagai entitas security guna menjamin perlindungan terhadap pelaku UMKM maupun konsumen. Perlindungan terhadap pelaku UMKM mencangkup beberapa aspek penting, antara lain perlindungan terhadap data toko, keamanan transaksi digital, kerahasiaan dagang, serta aspek legalitas usaha melalui perlindungan perizinan. Pelaku UMKM diharapkan dapat berinovasi tanpa perlu khawatir akan ancaman siber yang bisa mengganggu aktivitas bisnis mereka.

[44] Krisdian Rizki, "Perbandingan Hukum E-Commerce Indonesia Dengan Amerika Serikat" 2, no. 1 (2025): 423–35.

Perlindungan terhadap konsumen yang diberikan jaminan oleh LKSMPE juga menjadi prioritas yang tidak kalah penting, mencangkup perlindungan terhadap keamanan dan kerahasiaan data individual konsumen, memastikan bahwa situs e-commerce yang digunakan telah memiliki sertifikasi web yang sah (web certification), menjamin keamanan dalam proses transaksi digital, serta melindungi hak-hak konsumen dalam interaksi dagang secara elektronik. LKSMPE tidak hanya berfungsi untuk melindungi cyber crime, tapi juga menjadi solusi alternatif melalui website apabila terjadi sengketa bisnis antara e-commerce dan pengguna melalui dua mekanisme, yaitu virtual dan non-virtual. Mekanisme virtual memberikan informasi, edukasi, serta menjadi wadah pelaporan kasus cyber crime, khususnya bagi sengketa e-commerce guna menciptakan penanganan yang lebih efisien. Sedangkan, mekanisme non-virtual memiliki dua upaya penyelesaian melalui litigasi dan non-litigasi yang memiliki tugas untuk menindaklanjuti adanya laporan yang diterima oleh mekanisme virtual yang nantinya akan dijatuhi sanksi-sanksi.

Sanksi yang dijatuhkan melalui upaya non-litigasi apabila ada pihak yang melanggar kesepakatan pada hasil mediasi yang telah dilakukan, berupa denda administratif sebesar Rp 12.000.000.000. (Dua Belas Miliar Rupiah) serta penghapusan atau pemusnahan data pribadi. Sedangkan sanksi yang dijatuhkan melalui upaya litigasi dapat berupa denda administratif sebesar Rp 15.000.000.000.000 (Lima Belas Miliar Rupiah). Apabila sanksi litigasi yang telah ditetapkan tidak terpenuhi, maka akan dikenakan Dwangsom (uang paksa). Eksistensi LKSMPE dapat memperkuat cyber security sehingga konsumen merasa aman serta percaya dalam melakukan aktivitas belanja online. Implementasi perlindungan siber pada e-commerce melalui LKSMPE sejalan dengan Deterrence Theory yang menegaskan potensi kejahatan terutama kejahatan siber dapat dicegah dengan adanya lembaga yang mampu menimbulkan keraguan bagi pelaku kejahatan siber untuk melakukan tindakan ilegal, karena LKSMPE bertanggung jawab dalam memantau, melindungi, serta mengatur keamanan transaksi digital guna meningkatkan risiko yang dihadapi pelaku kejahatan siber.

Eksistensi Deterrence Theory memperkuat posisi negara dalam menjaga stabilitas serta kepercayaan publik terhadap sektor perdagangan digital. Hal ini telah dibuktikan dengan adanya implementasi Deterrence Theory yang digunakan oleh Pemerintah Amerika Serikat (AS) dalam pengembangan kebijakan strategis keamanan siber nasional yang mencangkup peningkatan sistem pertahanan digital, ancaman terhadap pelaku siber, serta kerja sama internasional untuk membangun efek jera secara global [45]. Keberhasilan implementasi ini dalam konteks kebijakan negara besar seperti AS menunjukkan bahwa Deterrence Theory relevan dan efektivitas teori ini, sehingga penerapannya dalam pembentukan LKSMPE menjadi

[45] O S Folorunsho, "Evaluating Cybersecurity Theories, Models, Standards and Frameworks," *Advances in Multidisciplinary and Scientific Research Journal Publication* 5, no. 4 (2019): 61–66, https://doi.org/10.22624/aims/bhi/v5n4p7.

langkah strategis yang sejalan dengan praktik internasional serta menjadi fondasi kuat bagi sistem perlindungan siber e-commerce nasional.

Perlindungan lainnya yang dapat berpotensi pada eksistensi cyber crime melalui PP PMSE berupa revisi penambahan pasal terkait lembaga perlindungan cyber crime di bidang e-commerce serta adanya sanksi bagi pelaku kejahatan. Regulasi yang tegas berguna untuk mengantisipasi dinamika serta kompleksitas kejahatan siber yang terus berkembang pada sektor perdagangan serta pemerintah dapat memberikan respons yang lebih tanggap terhadap potensi ancaman siber di bidang e-commerce. Oleh karena itu, penguatan regulasi melalui revisi penambahan pasal pada PP PMSE juga menjadi fondasi penting dalam menciptakan sektor perdagangan digital yang aman, terpercaya, serta berkelanjutan.

4. KESIMPULAN

Mengacu pada penelitian yang telah dipaparkan sebelumnya, maka penulis simpulkan hal-hal sebagai berikut:

1. Dalam era digital, kini UMKM berperan penting dalam menggerakkan roda perekonomian di Indonesia. Akan tetapi, perkembangan teknologi yang pesat ini juga membuka peluang ancaman terhadap keamanan siber. Lemahnya perlindungan data konsumen, minimnya literasi serta kurangnya regulasi dan pendampingan hukum membuat UMKM sangat rentan terhadap tindak kejahatan siber.
2. Kurangnya edukasi tentang keamanan siber, lemahnya regulasi yang berlaku, serta tidak adanya lembaga khusus yang menangani perlindungan UMKM secara langsung, serta belum optimalnya peran lembaga negara seperti BSSN, Kementerian Perdagangan, serta OJK dalam perlindungan konsumen menjadi tantangan besar untuk membangun ekosistem digital yang aman dan adil bagi pelaku UMKM.

REFERENSI

Ansori, Abdul Ghofur. 2016. *Lembaga Kenotariatan Indonesia: Perspektif Hukum Dan Etika, Cetakan Keempat*. Yogyakarta: UII Press.

B. Arief Sidharta, Mochtar Kusumaatmadja. 2013. *Pengantar Ilmu Hukum: Suatu Pengenalan Pertama Ruang Lingkup Berlakunya Ilmu Hukum*. Bandung: Alumni.

Darus, M.Luthfan Hadi. 2017. *Hukum Notariat Dan Tanggung Jawab Jabatan Notaris*. Yogyakarta: UII Press.

Fuady, Munir. 2005. *Perbuatan Melawan Hukum: Pendekatan Kontemporer*. Bandung: PT Citra Aditya Bakti.

Hadjon, Philipus M. 1987. *Perlindungan Hukum Bagi Rakyat Di Indonesia*. Surabaya: PT. Bina Ilmu.

Ibrahim, Johnny. 2007. *Teori & Metodologi Penelitian Hukum Normatif*. Malang: Bayumedia Publisher.A.S.E.A.N. "ASEAN Agreement on Electronic Commerce," 2019. https://agreement.asean.org/media/download/20190306035048.pdf.

Anak Agung Made Ayu Rai Lidya Astari, I.Nyoman Putu Budiartha, and Ni Made Puspasutari Ujianti. "Pengawasan Terhadap Transaksi Bisnis E-Commerce Dalam Mewujudkan Perlindungan Konsumen." *Jurnal Konstruksi Hukum* 1, no. 1 (2020): 38–43,. https://doi.org/10.22225/jkh.1.1.2126.38-43.

Annur, Cindy Mutia. "E-Commerce Indonesia Jadi Incaran, Peresetan Naik 6.000% Saat Pandemi." katadata.co.id, 2020. https://katadata.co.id/digital/e-commerce/5eeb755de99e5/e-commerce-indonesia-jadi-incaran-peretasan-naik-6000-saat-pandemi?utm_source.

Arbani, Muhammad. "Aspek Hukum Perlindungan Umkm Dalam Penjualan Di E-Commerce : Tantangan Dan Solusi Di Era Digital" 6, no. 2 (2025): 1166–75.

Ayudiana, Shofi. "Kemenkop UKM: 25,5 Juta UMKM Telah 'Go Digital,.'" www.antara.com, 2024. https://www.antaranews.com/berita/4397157/kemenkop-ukm-255-juta-umkm-telah-go-digital.

Christianingrum, Ratna. *Tantangan Penguatan Keamanan Siber Dalam Menjaga Stabilitas Keamanan*. Jakarta: Pusat Kajian Anggaran Keahlian DPR RI, 2021.

Damayanti, Fandani. "Hukum Perlindungan Konsumen Terhadap Barang Yang Tidak Sesuai Dengan Perjanjian E-Commerce," 2025.

Farras, Muhammad Naufal, and Harits Ar Rosyid. "Perdagangan Elektronik Pada Industri 4.0 Dan Society 5.0." *Jurnal Inovasi Teknologi Dan Edukasi Teknik* 3, no. 3 (2023): 122–27,. https://doi.org/10.17977/um068v3i32023p122-127.

Folorunsho, O S. "Evaluating Cybersecurity Theories, Models, Standards and Frameworks." *Advances in Multidisciplinary and Scientific Research Journal Publication* 5, no. 4 (2019): 61–66,. https://doi.org/10.22624/aims/bhi/v5n4p7.

Gunawan, Candra. "INFOGRAFIS:Nilai Ekonomi Digital Di Asia Tenggara, Indonesia Bakal Tumbuh Tiga Kali Lipat 2025," 2021. https://gokepri.com/infografis-nilai-ekonomi-digital-di-asia-tenggara-indonesia-bakal-tumbuh-tiga-kali-lipat-2025/.

Hafis, Faisal. "CEO Bukalapak Akui Kebocoran Data 13 Juta Akun Pengguna Tahun Lalu." Cyberheart.id, 2020. https://cyberthreat.id/read/6548/CEO-Bukalapak-Akui-Kebocoran-Data-13-Juta-Akun-Pengguna-Tahun-Lalu.

Indonesia. "Undang-Undang Dasar Negara Republik Indonesia Tahun 1945," 1945.

Indonesia, C N N. "Kronologi Lengkap 91 Juta Akun Tokopedia Bocor Dan Dijual." www.cnnindonesia.com, 2020. https://www.cnnindonesia.com/teknologi/20200503153210-185-499553/kronologi-lengkap-91-juta-akun-tokopedia-bocor-dan-dijual.

———. "Peretas Jual 1,2 Juta Data Pengguna Bhinneka.Com Di Dark Web." www.cnnindonesia.com, 2020. https://www.cnnindonesia.com/teknologi/20200511000424-185-501867/peretas-jual-12-juta-data-pengguna-bhinnekacom-di-dark-web.

Indonesia, CNN. "13 Juta Data Bocor Bukalapak Dijual Di Forum Hacker." www.cnnindonesia.com, 2020. https://www.cnnindonesia.com/teknologi/20200506065657-185-500477/13-juta-

data-bocor-bukalapak-dijual-di-forum-hacker.

Indonesia, Kementerian Koordinator Bidang Perekonomian Republik. "Dorong UMKM Naik Kelas Dan Go Export, Pemerintah Siapkan Ekosistem Pembiayaan Yang Terintegras," 2023. https://www.ekon.go.id/publikasi/detail/5318/dorong-umkm-naik-kelas-dan-go-export-pemerintah-siapkan-ekosistem-pembiayaan-yang-terintegrasi.

Indonesia, Republik. "Peraturan Pemerintah Republik Indonesia Nomor 80 Tahun 2019 Tentang Perdagangan Melalui Sistem Elektronik," n.d.

———. "Undang-Undang Nomor 8 Tahun 1999 Perlindungan Konsumen," n.d. https://peraturan.bpk.go.id/Home/Details/45288/uu-no-8-tahun-1999.

———. "Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik," n.d.

Kaharudin, and Zul Amirul Haq. *Kecerdasan Buatan Dan Aspek Perlindungan Hukum Di Era Digitalisasi*. Jakarta: Penada Kencana, 2024.

Kasali, Rhenald. *Change!: Pemimpin Dan Organisasi Dalam Pusaran Disrupsi*. Jakarta: Jakarta, 2020.

Komdigi. "Penggerak Inklusi Dan Pertumbuhan." komdigi.go.id, 2024. https://www.komdigi.go.id/berita/ekonomi-digital/detail/penggerak-inklusi-dan-pertumbuhan.

KumparanTECH. "Bukalapak Akui 13 Juta Data Yang Dijual Hacker Adalah Peretasan Di Maret 2019." www.kumparan.com, 2019. https://kumparan.com/kumparantech/bukalapak-akui-13-juta-data-yang-dijual-hacker-adalah-peretasan-di-maret-2019-1tMRTr1UR0G.

Maghfiroh, Fani Ma'sumatul. "Kolaborasi Salam Berbasis Crowdfunding." In *Proceedings of Islamic Economics, Business, and Philanthropy*, Vol. 2, 2023.

Marzuki, Peter Mahmud. *Penelitian Hukum*. Jakarta: Kencana Prenada Group, 2007.

Mayer, Robert N. "United Nations Guidelines for Consumer Protection." *Watchdogs and Whistleblowers: A Reference Guide to Consumer Activism*, 2015, 489–92.

Muslimin, J M. *Logika Dan Penalaran Hukum*. Tangerang Selatan: Pustaka Pedia, 2021.

"OECD Recommendation of the Council on Consumer Protection in E-Commerce." In *OECD Recommendation of the Council on Consumer Protection in E-Commerce*, 2016. https://doi.org/10.1787/9789264255258-en.

Padjarajani, Dr Siti. *Metodologi Penelitian Pendekatan Muldisipliner*. Gorontalo: Ideals Publishing, 2020.

Perdagangan, PSDI Kementerian. "Perdagangan Digital (E-Commerce) Indonesia Periode 2023," 2024.

Poniman, Hermaya Ompusunggu dan Poniman. "Studi Empiris Sistem Pembayaran Cashless Dan Cardless." *Owner* 8, no. 2 (2024): 1117–24. https://doi.org/https://doi.org/10.33395/owner.v8i2.2037.

Prayuti, Yuyut. "Dinamika Perlindungan Hukum Konsumen Di Era Digital: Analisis Hukum Terhadap Praktik E-Commerce Dan Perlindungan Data Konsumen Di

Indonesia." *Jurnal Interpretasi Hukum* 5, no. 1 (2024): 903–13,. https://doi.org/10.22225/juinhum.5.1.8482.903-913.

Privy. "Efisiensi Dan Pengguna Data Pengguna: 2 Hal Yang Harus Diperhatikan Di Era Revolusi Industri 4.0." privy.id, 2018. https://privy.id/blog/2-revolusi-industri-4/.

Putri, Deanne Destriani Firmansyah, and Muhammad Helmi Fahrozi. "Upaya Pencegahan Kebocoran Data Konsumen Melalui Pengesahan Ruu Perlindungan Data Pribadi (Studi Kasus E-Commerce Bhinneka.Com." *Borneo Law Review* 5, no. 1 (2021): 46–68,. https://doi.org/10.35334/bolrev.v5i1.2014.

Rahardjo, Sutjipto. *Ilmu Hukum*. Bandung: Alumni, 1982.

Republik Indonesia. "Majelis Permusyawaratan Rakyat, UUD Negara RI Tahun 1945.," n.d.

———. "Undang-Undang Republik Indonesia No. 7 Tahun 2014 Tentang Perdagangan," n.d. https://peraturan.bpk.go.id/Home/Details/38584/uu-no-7-tahun-2014.

RI, Kementerian Koordinator Bidang Perekonomian. "Perkuat Sektor Keamanan Siber, Indonesia Dan Australia Jalin Kerja Sama Pengembangan SDM," 2025. https://www.ekon.go.id/publikasi/detail/6186/perkuat-sektor-keamanan-siber-indonesia-dan-australia-jalin-kerja-sama-pengembangan-sdm.

Rizki, Krisdian. "Perbandingan Hukum E-Commerce Indonesia Dengan Amerika Serikat" 2, no. 1 (2025): 423–35.

Rizky, Demis. "Masa Depan Ekonomi Indonesia Tak Secerah Dahulu Kala." www.cnbcindonesia.com, 2023. https://www.cnbcindonesia.com/tech/20231102074541-37-485689/masa-depan-ekonomi-digital-indonesia-tak-secerah-dahulu-kala.

Rokilah, Rokilah. "Dinamika Negara Hukum Indonesia: Antara Rechtsstaat Dan Rule Of Law." *Nurani Hukum* 2, no. 1 (2020): 12. https://doi.org/10.51825/nhk.v2i1.8167.