E-ISSN: 3031-8629
P-ISSN: 3032-3258
Halaman 54-75
Volume 2 Nomor 2 Tahun 2025

Peran Pemerintah Dalam Membangun Kebijakan Keamanan Siber Untuk Meningkatkan Kepercayaan Pengguna *E-Commerce* Di Indonesia

Tri Ginanjar Laksana[1]
[1]Program Studi Teknik Informatika, Universitas Bhayangkara Jakarta Raya
e-mail: tri.ginanjar.laksana@dsn.ubharajaya.ac.id

Abstrak

Dalam beberapa tahun terakhir, industri e-commerce Indonesia telah berkembang dengan cepat. Banyak orang di industri ini beralih dari belanja secara langsung ke belanja online. Namun, dengan kemajuan ini muncul masalah baru, terutama yang berkaitan dengan keamanan dan kepercayaan pengguna. Tujuan dari penelitian ini adalah untuk membahas bagaimana hukum keamanan siber yang didukung pemerintah berkontribusi pada peningkatan kepercayaan pelanggan Indonesia pada e-commerce. Studi ini menggunakan metode kualitatif untuk memeriksa teori kepercayaan konsumen. Data dikumpulkan melalui wawancara semi terstruktur dan studi literatur. Klasifikasi dan interpretasi kualitatif adalah bagian dari analisis data. Selama penelitian, pertimbangan etis digunakan untuk menghindari bias dan memastikan persetujuan responden, privasi, dan kerahasiaan. Studi menunjukkan bahwa kepercayaan sangat penting untuk kesuksesan industri e-commerce di era digital yang semakin maju. Keamanan siber yang didukung pemerintah membuat orang percaya satu sama lain. Hukuman keamanan siber yang didukung pemerintah memainkan peran penting dalam meningkatkan kepercayaan pada e-commerce di Indonesia karena membuat pengguna merasa aman dan terlindungi saat mereka melakukan transaksi online. Bisnis e-commerce juga dapat memperoleh manfaat dari hukum ini dengan mematuhi persyaratan kepatuhan dan meningkatkan keamanan siber mereka.

Kata kunci: Pemerintah; Keamanan Cyber; Hukum; Perdagangan Elektronik; Percaya; Ancaman;

E-ISSN: 3031-8629
P-ISSN: 3032-3258
Halaman 54-75
Volume 2 Nomor 2 Tahun 2025

Abstract

The e-commerce industry in Indonesia has seen substantial expansion in recent years. Companies in this sector are seeing a significant increase in the shift from traditional brick-and-mortar retail to online shopping. However, the progress has also presented other obstacles, namely in terms of security and customer trust. This research investigates the need of government-backed cybersecurity laws in enhancing the confidence of Indonesian consumers in the realm of electronic commerce. This research investigates the fundamentals of consumer trust theory via the use of a qualitative approach. The data was collected via semi-structured interviews and a comprehensive examination of available literature. Data analysis is the systematic classification and interpretation of data using qualitative criteria. The study was carried out with a significant focus on ethical considerations to mitigate any bias and ensure the consent, privacy, and confidentiality of the participants. The survey results suggest that trust is a crucial factor in the success of the e-commerce industry in a constantly changing digital era. State-sponsored cybersecurity measures bolster trust. E-commerce firms may also benefit from this law by complying with the requirements and improving their cybersecurity procedures. Therefore, it is imperative to enact government-backed cybersecurity laws in order to bolster trust in e-commerce.

Keywords : *Government; cyber security; laws; e-commerce; trust; Threats;*

LATAR BELAKANG

Penelitian ini membahas kebijakan terkait peran pemerintah dalam membangun hukum keamanan siber untuk meningkatkan kepercayaan pengguna e-commerce di Indonesia, menggunakan perspektif hukum siber (*Cyber Law*) dengan teori kepercayaan konsumen. Kepercayaan adalah faktor kunci dalam kesuksesan industri e-commerce[1],[2]. Bisnis e-commerce harus memastikan bahwa pelanggan merasa aman dan terlindungi saat berbelanja online karena mereka akan enggan untuk melakukannya jika mereka merasa tidak aman atau tidak yakin dengan keamanan platform tersebut[2]. Secara keseluruhan, kepercayaan adalah dasar dari hubungan

yang berhasil antara platform e-commerce dan pelanggan[3]. Tanpa kepercayaan, pelanggan mungkin tidak mau bertransaksi, dan ini dapat menghambat pertumbuhan bisnis e-commerce[4]. Oleh karena itu, platform e-commerce harus terus berusaha untuk menumbuhkan dan mempertahankan kepercayaan pelanggan melalui berbagai cara, seperti menjaga keamanan data mereka dan memberikan pengalaman pengguna yang luar biasa[1],[5].

Pemerintah bertanggung jawab atas keamanan industri e-commerce[7]. Mereka bertanggung jawab untuk membuat kebijakan dan regulasi yang melindungi pengguna dari ancaman keamanan online[8],[9]. Selain itu, pemerintah juga bekerja sama dengan badan-badan keamanan siber untuk melacak dan mengatasi serangan siber yang terjadi dalam e-commerce. Mengidentifikasi orang yang melakukan kejahatan siber dan mengambil tindakan hukum terhadap mereka adalah bagian dari ini. Pemerintah membantu pengguna merasa lebih percaya dan aman saat mereka melakukan transaksi online. Pemerintah dapat membangun lingkungan digital yang lebih aman dan terpercaya, mendorong pertumbuhan ekonomi, dan melindungi hak-hak pengguna.

Beberapa ancaman umum yang dihadapi oleh pengguna e-commerce termasuk pencurian identitas, penipuan online, dan serangan siber lainnya[8],[6],[10]. Hukum keamanan siber yang didukung oleh pemerintah, misalnya, tidak dibuat untuk mengatasi ancaman-ancaman ini dan mengharuskan bisnis e-commerce untuk memberikan perlindungan data yang memadai kepada pengguna, termasuk enkripsi data dan perlindungan terhadap serangan siber[11]. Selain itu, hukum ini juga menetapkan sanksi tegas bagi perusahaan yang tidak memenuhi syarat[12],[13].

Ada beberapa studi kasus yang menunjukkan keberhasilan implementasi hukum keamanan siber yang didukung oleh pemerintah di Indonesia. Salah satu contoh sukses adalah implementasi Undang-Undang Perlindungan Data Pribadi (UU PDP)[24],[25]. UU ini bertujuan untuk melindungi data pribadi pengguna dan memastikan bahwa data tersebut tidak disalahgunakan. Sejak diberlakukannya UU PDP, banyak bisnis e-commerce yang meningkatkan keamanan data mereka dan

melindungi privasi pengguna dengan lebih baik[26],[27]. Ini telah meningkatkan kepercayaan pengguna pada platform e-commerce di Indonesia[28]. Penting untuk dicatat bahwa keberhasilan dalam keamanan siber tidak hanya tergantung pada peraturan dan undang-undang, tetapi juga pada kemampuan untuk mengimplementasikan, mematuhi, dan memantau kepatuhan terhadap standar keamanan siber[15]. Selain itu, isu keamanan siber terus berkembang, dan pemerintah perlu beradaptasi dan memperbarui kebijakan mereka untuk mengatasi ancaman yang muncul[29].

Bisnis e-commerce harus memenuhi persyaratan kepatuhan tertentu untuk mematuhi undang-undang keamanan siber yang didukung pemerintah[30]. Salah satu persyaratan utama adalah melindungi data pengguna dengan baik[31]. Bisnis harus menerapkan langkah-langkah keamanan seperti enkripsi data, firewall, dan perlindungan terhadap serangan siber, serta mematuhi peraturan perlindungan data pemerintah, seperti UU PDP[32]. Dengan melakukan hal ini, bisnis e-commerce dapat meningkatkan kepercayaan pengguna dan memastikan bahwa data mereka aman[33]. Memahami dan mematuhi persyaratan kepatuhan ini akan membantu mematuhi undang-undang dan membuat lingkungan pelanggan aman dan terpercaya. Ini akan meningkatkan reputasi dan keberlanjutan bisnis e-commerce[34].

Ada berbagai sumber daya dan dukungan yang tersedia untuk membantu bisnis e-commerce meningkatkan keamanan siber mereka[14]. Pemerintah membuat standar dan pedoman tentang praktik keamanan siber yang baik, dan ada juga lembaga independen yang menyetujui bisnis yang memenuhi persyaratan tertentu[35]. Selain itu, bisnis dapat memperoleh pemahaman yang lebih baik tentang ancaman keamanan siber dan cara menanganinya dengan mengikuti pelatihan dan seminar[15]. Dengan menggunakan sumber daya dan dukungan ini, bisnis e-commerce dapat memperkuat keamanan siber mereka dan menjaga kepercayaan pengguna[36]. Kombinasi dari sumber daya ini dapat membantu bisnis membangun dan mempertahankan program keamanan siber yang kokoh. Penting

untuk terus mengamati kemajuan dalam keamanan siber dan menyesuaikan taktik untuk menghadapi ancaman baru.

METODE

Penelitian ini menggunakan metodologi penelitian doktrinal, menggunakan pendekatan undang-undang dan konseptual. Dokumen hukum yang digunakan dalam penelitian ini meliputi sumber primer, sekunder, dan tersier. Bahan hukum teknis dikumpulkan melalui tinjauan literatur (studi dokumentasi) dan pencarian online. Pemeriksaan dokumen hukum dalam penelitian bersifat deskriptif analisis.

HASIL DAN PEMBAHASAN

A. Pentingnya Kepercayaan dalam Menggunakan e-Commerce

Dalam industri e-commerce, kepercayaan sangat penting karena melibatkan transaksi online di mana pelanggan harus memberikan informasi pribadi dan keuangan mereka untuk melakukan pembelian[37]. Untuk alasan berikut, kepercayaan sangat penting dalam e-commerce: Keamanan Finansial: Untuk melakukan pembelian melalui internet, pelanggan seringkali diminta untuk memberikan detail keuangan seperti nomor kartu kredit mereka[38]. Kepercayaan tinggi pada platform e-commerce dapat membantu memastikan bahwa data ini dikelola dengan aman dan tidak disalahgunakan[39]. Perlindungan Data Pribadi: Dalam e-commerce, informasi pribadi seperti alamat pengiriman dan nomor telepon sering dibutuhkan[40]. Anda harus yakin dapat melindungi data pribadi pelanggan Anda agar tidak jatuh ke tangan yang tidak diinginkan atau digunakan untuk tujuan yang tidak diinginkan. Pengalaman Pengguna yang Positif: Pelanggan yang percaya bahwa suatu platform aman dan kredibel akan lebih nyaman berbelanja dan berinteraksi dengan situs web atau aplikasi e-commerce[24]. Ulasan dan Reputasi: Ulasan dan reputasi positif dari pelanggan sebelumnya dapat meningkatkan kepercayaan pelanggan potensial pada platform e-commerce. Ketepatan Pengiriman dan Kualitas Produk: Kemampuan sebuah platform untuk memberikan produk sesuai dengan deskripsi dan dalam waktu yang dijanjikan meningkatkan kepercayaan pelanggan. Ketepatan pengiriman dan kualitas produk yang baik dapat meningkatkan

kepercayaan pelanggan. Kebijakan Pengembalian dan Pelayanan Pelanggan: Kejelasan dan transparansi dalam kebijakan pengembalian barang dan layanan pelanggan yang responsif adalah bagian penting dari kepercayaan[41]. Konsumen harus yakin bahwa mereka dapat dengan mudah menghubungi dan mendapatkan bantuan jika terjadi masalah. Perlindungan Hukum: Konsumen harus yakin bahwa mereka dilindungi dari pelanggaran hukum dalam transaksi online. Akibatnya, kepatuhan platform terhadap peraturan dan kebijakan perlindungan konsumen juga dapat meningkatkan kepercayaan. Inovasi dan Keandalan Teknologi: Keandalan teknologi dan kepercayaan juga terkait. Kepercayaan pelanggan terhadap kemampuan platform e-commerce untuk memberikan layanan yang handal dapat meningkat berkat inovasi dan teknologi yang canggih.

B. Gambaran Umum tentang Hukum Keamanan Siber yang Didukung Pemerintah

Hukum keamanan siber yang didukung pemerintah dapat berbeda dari negara ke negara[42]. Sementara beberapa negara memiliki kerangka hukum yang lengkap untuk menangani masalah keamanan siber, yang lain masih membuatnya[6]. Di bawah ini adalah beberapa komponen umum yang mungkin tercakup dalam hukum keamanan siber yang didukung pemerintah: Undang-Undang Perlindungan Data: Undang-undang ini mengatur perlindungan data pribadi. Ini dapat mencakup peraturan tentang pengumpulan, penyimpanan, dan pengolahan data pribadi oleh perusahaan dan lembaga pemerintah. Undang-undang Anti-Cybercrime: Beberapa negara memiliki undang-undang khusus yang menangani kejahatan siber seperti serangan peretasan, pencurian data, penipuan online, dan kejahatan siber lainnya[43]. Undang-undang ini menyediakan kerangka hukum untuk penegakan hukum terhadap pelaku kejahatan siber. Pembentukan dan Pengawasan Otoritas Keamanan Siber: Beberapa negara menciptakan otoritas atau lembaga khusus yang menangani keamanan siber. Otoritas ini mungkin bertanggung jawab untuk mengembangkan kebijakan, membuat aturan, dan mengawasi berbagai industri dalam hal penerapan keamanan siber. Pentingnya Kepatuhan dan Pelaporan: Hukum keamanan siber seringkali menekankan bahwa organisasi harus mematuhi peraturan keamanan tertentu. Selain itu, undang-undang mungkin memerlukan organisasi

untuk melaporkan kepada pihak berwenang jika terjadi masalah keamanan siber. Perlindungan Infrastruktur Kritis: Beberapa negara memiliki hukum yang melindungi infrastruktur kritis, seperti sistem listrik, air, atau transportasi, dari ancaman keamanan siber. Ini mungkin mencakup peraturan keamanan yang ketat dan tindakan pencegahan. Kerjasama Internasional: Beberapa hukum negara mengenai keamanan siber mencakup ketentuan tentang kerja sama internasional dalam memerangi serangan siber lintas batas. Ini dapat mencakup pertukaran data, bantuan hukum, dan kolaborasi di seluruh dunia. Pelatihan dan Sertifikasi Keamanan Siber: Hukum mungkin ada di beberapa negara yang mendukung profesional yang bekerja di bidang ini untuk menerima pelatihan dan sertifikasi dalam bidang keamanan siber. Hukuman dan Denda: Peraturan keamanan siber biasanya mencakup sanksi, denda, dan hukuman pidana untuk pelanggaran keamanan siber, dengan tujuan memberikan tekanan hukum dan ekonomi terhadap pelaku kejahatan siber.

C. Peran Pemerintah dalam Memastikan Keamanan Pengguna

Mengingat perkembangan teknologi informasi dan ketergantungan masyarakat pada dunia digital, peran pemerintah dalam menjaga keamanan pengguna, terutama dalam hal keamanan siber, sangat penting. Beberapa peran penting yang dimainkan oleh pemerintah dalam hal ini termasuk: Pembentukan Kebijakan dan Hukum: Pemerintah bertanggung jawab untuk menetapkan kebijakan dan undang-undang yang membentuk kerangka hukum untuk keamanan siber. Ini termasuk undang-undang perlindungan data, undang-undang anti-cybercrime, dan peraturan terkait lainnya. Pembentukan Otoritas Keamanan Siber: Di tingkat nasional, pemerintah dapat membentuk otoritas keamanan siber atau badan regulasi khusus untuk mengawasi dan mengelola keamanan siber. Untuk menangani ancaman keamanan siber, otoritas ini dapat memberikan pedoman, rekomendasi, dan koordinasi tindakan. Pendidikan dan Kesadaran Publik: Pemerintah dapat berperan besar dalam meningkatkan kesadaran publik tentang praktik keamanan siber yang baik. Kampanye pendidikan dan informasi dapat membantu pengguna memahami risiko dan ancaman. Perlindungan Infrastruktur Kritis: Pemerintah bertanggung jawab

untuk melindungi infrastruktur penting, seperti sistem energi, transportasi, dan keuangan, dari serangan siber. Ini berarti mengembangkan dan menerapkan standar keamanan yang ketat. Kerjasama Internasional: Kerjasama internasional sangat penting di dunia yang semakin terhubung. Pemerintah harus bekerja sama dengan negara lain untuk membuat standar keamanan internasional, berbagi data, dan menangani ancaman siber lintas batas. Penegakan Hukum dan Kepatuhan: Pemerintah bertanggung jawab untuk melindungi keamanan siber dan mengambil tindakan terhadap mereka yang melakukan kejahatan siber. Ini termasuk melakukan penyelidikan, penuntutan, dan menerapkan sanksi terhadap individu atau kelompok yang terlibat dalam kejahatan siber. Pengembangan Riset dan Teknologi Keamanan: Pemerintah dapat memberikan dukungan untuk penelitian dan pengembangan dalam bidang keamanan siber. Ini termasuk menciptakan alat deteksi serangan, teknologi keamanan, dan inovasi keamanan lainnya untuk melawan ancaman baru. Pengawasan dan Audit Keamanan: Pemerintah dapat mengawasi dan mengaudit organisasi, terutama di sektor kritis, untuk memastikan bahwa mereka mematuhi peraturan keamanan yang ditetapkan dan melindungi data dengan benar. Respon Krisis: Untuk menangani serangan siber besar-besaran atau insiden keamanan yang signifikan, pemerintah harus memiliki rencana respons krisis yang efektif. Ini melibatkan kerja sama antara lembaga pemerintah dan swasta, serta entitas lain yang berhubungan dengan masalah ini.

D. Ancaman Umum dalam E-commerce dan Bagaimana Hukum Mengatasinya

E-commerce menjadi target berbagai ancaman keamanan siber yang dapat membahayakan bisnis, data pelanggan, dan kepercayaan konsumen[26],[44]. Berikut adalah beberapa ancaman umum dalam e-commerce dan bagaimana hukum dapat membantu mengatasinya: 1. Pencurian Identitas dan Penipuan: Ancaman: Pencuri dapat mencuri data identitas pelanggan atau melakukan penipuan dengan menggunakan informasi palsu. Hukum: Hukum keamanan siber dapat mengatur perlindungan data pribadi, memberikan sanksi bagi pelaku pencurian identitas, dan memerlukan tindakan keamanan tambahan seperti otentikasi dua faktor. 2. Serangan Malware: Ancaman: Serangan malware dapat menyebabkan kerusakan pada sistem

e-commerce, mencuri informasi sensitif, atau mengakibatkan layanan tidak tersedia. Hukum: Hukum dapat memerlukan pemantauan dan perlindungan terhadap malware, serta menetapkan sanksi bagi mereka yang terlibat dalam penyebaran malware. 3. Serangan DDoS (Distributed Denial of Service): Ancaman: Serangan DDoS dapat menyebabkan situs web e-commerce menjadi tidak tersedia, mengakibatkan gangguan operasional dan kerugian finansial. Hukum: Hukum keamanan siber dapat menetapkan sanksi bagi pelaku serangan DDoS, dan bisnis dapat mengambil langkah-langkah untuk memitigasi dampak serangan ini. 4. Pelanggaran Data: Ancaman: Penyusup dapat mencuri data pelanggan, seperti informasi kartu kredit, yang dapat menyebabkan kerugian finansial dan reputasi. Hukum: Hukum perlindungan data mengatur bagaimana perusahaan harus melindungi dan mengelola data pelanggan. Pelanggaran hukum ini dapat mengakibatkan sanksi dan tuntutan hukum. 5. Phishing: Ancaman: Serangan phishing melibatkan upaya untuk mendapatkan informasi sensitif dengan menyamar sebagai entitas tepercaya. Hukum: Hukum dapat melarang praktik phishing dan memberikan sanksi bagi pelaku. Bisnis juga dapat memberikan edukasi kepada pelanggan tentang cara mengidentifikasi upaya phishing. 6. Keamanan Sistem Pembayaran: Ancaman: Penjahat dapat mencoba mencuri informasi pembayaran, mengakibatkan kerugian finansial bagi konsumen dan bisnis. Hukum: Hukum keamanan pembayaran mengatur praktik-praktik yang aman dan memerlukan perlindungan data pembayaran. Penyelewengan hukum ini dapat mengakibatkan sanksi dan tanggung jawab hukum. 7. Kehilangan Aset Digital: Ancaman: Bisnis e-commerce dapat mengalami kehilangan aset digital, termasuk desain unik, hak cipta, atau data pelanggan. Hukum: Hukum hak kekayaan intelektual melibatkan perlindungan terhadap kekayaan intelektual bisnis. Pelanggaran hak kekayaan intelektual dapat dikenai sanksi hukum. 8. Ketidakpatuhan Terhadap Standar Keamanan: Ancaman: Bisnis yang tidak mematuhi standar keamanan tertentu dapat menjadi rentan terhadap serangan dan pelanggaran data. Hukum: Hukum keamanan siber dapat mewajibkan bisnis untuk mematuhi standar keamanan tertentu dan memberikan sanksi jika tidak memenuhi persyaratan ini. 9. Ketidakpatuhan

Terhadap Hak Privasi: Ancaman: Pengumpulan dan pengolahan data pelanggan tanpa izin dapat melanggar privasi individu. Hukum: Hukum privasi data dan peraturan seperti GDPR menetapkan standar untuk pengelolaan data pelanggan dan memberikan hak kepada individu untuk mengontrol informasi pribadi mereka. 10. Respons Terhadap Insiden Keamanan: - **Ancaman:** Ketidakmampuan merespons dengan cepat terhadap insiden keamanan dapat memperburuk dampak kerugian. - **Hukum:** Hukum dapat mengatur kewajiban untuk melaporkan insiden keamanan dengan cepat dan memberikan pedoman untuk respons dan pemulihan. Menggabungkan praktik keamanan yang baik dengan kepatuhan hukum dapat membantu bisnis e-commerce melindungi diri dari ancaman dan membangun kepercayaan pelanggan. Bisnis perlu secara aktif mengikuti perkembangan hukum keamanan siber dan selalu meningkatkan langkah-langkah keamanan mereka sesuai dengan risiko yang berkembang.

E. Manfaat Hukum Keamanan Siber yang Didukung Pemerintah bagi Bisnis dan Konsumen

Hukuman keamanan siber yang didukung pemerintah dapat sangat membantu bisnis dan pelanggan[45]. Berikut adalah beberapa keuntungan penting: Manfaat untuk Bisnis: Perlindungan Terhadap Ancaman Hukum: Peraturan keamanan siber mengatur perlindungan data, tanggung jawab dalam pelanggaran, dan sanksi terhadap pelaku kejahatan siber. Kepatuhan dan Reputasi: Mengikuti hukum keamanan siber membantu bisnis mengikuti peraturan dan peraturan pemerintah. Kepatuhan ini dapat meningkatkan reputasi perusahaan, memberi pelanggan kepercayaan, dan menghindari sanksi hukum. Perlindungan Data Pelanggan: Peraturan mengatur bagaimana mengolah dan melindungi data pelanggan. Ini membantu perusahaan menghindari pelanggaran privasi dan kehilangan kepercayaan pelanggan karena penanganan data yang tidak aman. Kerjasama dengan Pihak Ketiga: Bisnis dapat bekerja sama dengan penyedia layanan keamanan siber pihak ketiga tanpa mengambil risiko hukum yang signifikan jika ada kerangka hukum yang jelas. Ini memiliki potensi untuk meningkatkan kemampuan keamanan siber mereka. Peningkatan Kesadaran dan Pelatihan: Peraturan keamanan siber

seringkali menuntut agar karyawan diberi pelatihan dan kesadaran tentang keamanan. Ini dapat membantu mengurangi kemungkinan serangan siber yang berasal dari kelalaian manusia. Pengurangan Risiko dan Kerugian Finansial: Kepatuhan terhadap hukum keamanan siber dapat membantu bisnis mengidentifikasi dan mengurangi risiko serangan siber. Ini dapat mengurangi kemungkinan kerugian finansial karena serangan siber, pemulihan data, dan kehilangan bisnis. Keamanan dan Kontinuitas Operasional: Bisnis yang mematuhi hukum keamanan siber cenderung memiliki sistem dan prosedur yang lebih aman untuk memastikan kontinuitas operasional dan melindungi aset bisnis dari kerusakan atau kehilangan.

Manfaat untuk Konsumen: Perlindungan Privasi dan Data: Hukum keamanan siber mencegah penggunaan data pribadi konsumen yang tidak sah atau tidak etis[46]. Ini membuat konsumen merasa aman tentang privasi data mereka. Hak Kontrol Data: Hukum keamanan siber biasanya memberikan konsumen hak untuk mengontrol data pribadi mereka, termasuk hak untuk mengetahui bagaimana data digunakan, memberikan izin, dan menarik izin kapan pun diperlukan. Kepercayaan dan Transparansi: Hukum yang mendukung keamanan siber dapat membuat bisnis lebih transparan tentang keamanan dan perlindungan data[47]. Ini membuat pelanggan percaya pada bisnis e-commerce[48]. Pengaduan dan Penyelesaian Sengketa: Jika konsumen merasa hak privasi atau keamanan mereka dilanggar, hukum memberi mereka kerangka kerja untuk mengajukan pengaduan. Ini memberikan mekanisme penyelesaian sengketa yang adil dan transparan[49]. Kesadaran Keamanan Digital: Meningkatkan kesadaran konsumen tentang keamanan digital penting untuk mematuhi hukum keamanan siber. Ini dapat mengajarkan pelanggan keterampilan dan pengetahuan untuk melindungi diri secara online. Perlindungan terhadap Penipuan dan Pencurian Identitas: Dengan memberikan dasar hukum untuk penuntutan terhadap pelaku kejahatan siber, hukum dapat memperkuat perlindungan konsumen terhadap penipuan dan pencurian identitas. Akses Informasi yang Jelas: Peraturan keamanan siber dapat mewajibkan bisnis untuk memberi tahu pelanggan mereka tentang praktik keamanan dan

pengelolaan data yang jelas dan mudah dipahami. Dengan menerapkan hukum keamanan siber yang kuat, pemerintah dapat membuat e-commerce lebih aman dan dapat dipercaya. Ini meningkatkan kepercayaan, mengurangi ancaman siber, dan mendorong pertumbuhan ekonomi digital.

F. Studi Kasus tentang Implementasi Hukum Keamanan Siber yang Sukses di Indonesia

Beberapa inisiatif dan pencapaian, termasuk Badan Siber dan Sandi Negara (BSSN), dapat digunakan untuk mengukur kemajuan dalam penerapan hukum keamanan siber yang didukung oleh pemerintah Indonesia. Berikut ini adalah beberapa faktor yang menunjukkan keberhasilan implementasi hukum keamanan siber di Indonesia: 1. Pembentukan Badan Siber dan Sandi Negara (BSSN): BSSN dibentuk pada tahun 2. Program Nasional Keamanan Siber: Peluncuran Program Nasional Keamanan Siber menunjukkan janji pemerintah untuk meningkatkan kemampuan keamanan siber nasional. Program ini mencakup upaya untuk menemukan dan melindungi infrastruktur kritis serta meningkatkan kemampuan untuk menghadapi ancaman siber. 3. Kerjasama Internasional: Terlibat dalam kerjasama internasional membantu pertukaran informasi, pelatihan, dan koordinasi tindakan terhadap ancaman siber lintas batas. Ini menegaskan posisi Indonesia dalam menghadapi ancaman keamanan siber internasional. 4. Penyelenggaraan Acara dan Kampanye Kesadaran Keamanan Siber: Pemerintah dan BSSN sering mengadakan acara dan kampanye untuk meningkatkan kesadaran masyarakat tentang keamanan siber. Langkah-langkah seperti ini dapat membantu masyarakat dan bisnis lebih memahami ancaman siber dan mengambil tindakan pencegahan. 5. Ketentuan Keamanan Siber dalam Undang-Undang ITE: Ketentuan dalam Undang-Undang ITE menunjukkan betapa efektifnya undang-undang keamanan siber; ini memberikan dasar hukum untuk menangani kejahatan siber dan memberlakukan sanksi terhadap pelakunya. 6. Peran Pemerintah dalam Pelatihan dan Sertifikasi Keamanan Siber: Upaya pemerintah dan lembaga terkait untuk meningkatkan pelatihan dan sertifikasi keamanan siber dapat meningkatkan kapasitas profesional di bidang ini. 7. Peningkatan Kesadaran dan Peran Swasta: Peningkatan kesadaran

akan keamanan siber telah meningkatkan kesadaran masyarakat umum dan bisnis. Jumlah orang yang mendapatkan sertifikasi keamanan siber telah menunjukkan hasilnya.

G. Persyaratan Kepatuhan bagi Bisnis E-commerce

Di bidang e-commerce, kepatuhan sangat penting untuk melindungi pelanggan[50], mempertahankan kepercayaan pelanggan, dan mematuhi undang-undang yang berlaku. Persyaratan kepatuhan mungkin berbeda-beda menurut yurisdiksi, tetapi berikut adalah beberapa aspek umum yang harus dipertimbangkan oleh bisnis e-commerce: 1. Perlindungan Data dan Privasi: Persyaratan: Melibatkan pengumpulan, penyimpanan, dan pengolahan data pelanggan sesuai dengan undang-undang privasi yang berlaku, seperti 2. Transparansi Harga dan Informasi Produk: Persyaratan: Memberikan informasi harga yang jelas, termasuk biaya tambahan jika ada, dan deskripsi produk yang akurat. Tindakan: Menampilkan harga dengan jelas, termasuk pajak dan biaya pengiriman. Memberikan deskripsi produk yang rinci dan gambar yang akurat. 3. Keamanan Transaksi dan Pembayaran: Persyaratan: Mengamankan data pembayaran pelanggan dan menyediakan transaksi yang aman. Tindakan: Menggunakan protokol keamanan seperti SSL, menawarkan opsi pembayaran yang aman, dan mematuhi standar keamanan pembayaran kartu kredit, seperti PCI DSS. 4. Hak Konsumen dan Kebijakan Pengembalian: Persyaratan: Memberikan hak konsumen, termasuk kebijakan pengembalian barang dan garansi; Tindakan: Memberikan informasi yang jelas tentang kebijakan pengembalian, pertukaran, dan garansi. memastikan bahwa konsumen memiliki akses yang mudah ke hak mereka. 5. Kepatuhan Pajak dan Bea Cukai: Persyaratan: Mematuhi undang-undang pajak dan bea cukai yang berlaku di wilayah operasi; Tindakan: Melakukan perhitungan dan pemungutan pajak sesuai dengan regulasi setempat; Memastikan pemenuhan kewajiban bea cukai untuk pengiriman internasional. 6. Ketentuan Kontrak dan Hukum: Persyaratan: Membuat ketentuan dan ketentuan pengguna yang sah dan mengikat. Tindakan: Memastikan bahwa kontrak dan ketentuan yang digunakan sah dan dapat diterapkan dengan menyediakan dokumen hukum seperti Syarat dan Ketentuan, Kebijakan Privasi, dan

Kebijakan Pengembalian. 7. Kepatuhan dengan Undang-Undang Periklanan dan Promosi: Persyaratan: Mengikuti peraturan periklanan dan promosi. Tindakan: Membuat kampanye iklan yang jujur dan transparan. Menghindari periklanan yang dapat dianggap palsu. 8. Aksesibilitas dan Keterlibatan Pelanggan: Persyaratan: memastikan bahwa situs web atau aplikasi dapat diakses oleh semua orang, termasuk individu dengan kebutuhan khusus; Tindakan: menyediakan antarmuka yang dapat diakses, termasuk deskripsi alternatif untuk elemen visual. Menjawab keluhan dan pertanyaan pelanggan dengan cepat dan efektif. 9. Pelaporan dan Respons Keamanan Siber: Persyaratan: Persiapan dan respons terhadap insiden keamanan siber. Tindakan: Menetapkan kebijakan keamanan siber, melakukan audit keamanan, dan merespons segera jika terjadi pelanggaran keamanan. 10. Kepatuhan Terhadap Regulasi E-commerce Lokal: Persyaratan: Memahami dan mematuhi peraturan e-commerce yang berlaku di setiap yurisdiksi tempat bisnis beroperasi. Tindakan: Mempelajari dan memahami persyaratan hukum e-commerce setempat dan memastikan bahwa bisnis mematuhi peraturan tersebut.

H. Sumber daya dan Dukungan yang Tersedia untuk Meningkatkan Keamanan Siber

Meningkatkan keamanan siber berarti menerapkan tindakan preventif, mendapatkan pelatihan, dan menggunakan sumber daya yang tepat. 1. Badan Keamanan Siber dan Otoritas Pemerintah: Badan Siber dan Sandi Negara (BSSN). BSSN atau lembaga serupa di negara Anda dapat memberikan pedoman, instruksi, dan dukungan teknis tentang keamanan siber. Selain itu, mereka memiliki kemampuan untuk memberikan pelatihan dan memberikan informasi terkini tentang ancaman keamanan. 2. Pedoman dan Standar Keamanan: ISO/IEC 27001 adalah standar internasional yang mengatur standar sistem manajemen keamanan informasi. NIST Cybersecurity Framework: Kerangka kerja yang dibuat oleh National Institute of Standards and Technology (NIST) Amerika Serikat untuk meningkatkan keamanan siber. 3. Pelatihan Keamanan Siber: Sertifikasi Keamanan Siber: Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH), dan CompTIA Security+ adalah sertifikasi yang dapat membantu Anda meningkatkan keterampilan keamanan siber. Kursus Online: Kursus keamanan siber dapat diakses

secara fleksibel melalui platform pelatihan online seperti SANS Institute, Coursera, dan edX. 4. Alat Keamanan: Firewall dan Antivirus adalah alat dasar yang membantu melindungi sistem dari ancaman siber. Anti-Malware dan Anti-Spyware melindungi sistem dari malware dan perangkat lunak mata-mata. Sistem Deteksi Intrusi (IDS) dan Sistem Pencegahan Intrusi (IPS): Mendeteksi dan mencegah serangan siber. 5. Layanan Keamanan Cloud: Layanan Keamanan Cloud: Layanan keamanan cloud bawaan disediakan oleh platform cloud seperti AWS, Azure, dan Google Cloud. 7. Publikasi dan Riset Keamanan: White Papers: Baca white papers dari lembaga penelitian dan penyedia keamanan siber untuk mendapatkan wawasan tentang teknologi dan praktik keamanan terbaru. Konferensi dan Seminar: Hadiri konferensi dan seminar tentang keamanan siber untuk mendengarkan ahli dan memperluas jaringan Anda. 8. Layanan Keamanan Pihak Ketiga: Penilaian Keamanan Pihak Ketiga: Perusahaan keamanan siber pihak ketiga melakukan evaluasi keamanan sistem dan memberikan saran untuk perbaikan. Penetrasi (Pen Testing): Perusahaan keamanan siber pihak ketiga melakukan uji keamanan sistem untuk menemukan celah. 9. Blogs dan Situs Web tentang Keamanan Siber: Ikuti blog keamanan siber yang dikelola oleh para ahli untuk mendapatkan wawasan tentang tren dan berita terbaru. 10. Kemitraan Industri dan Organisasi: Bermitra dengan Lembaga Keamanan: Untuk mendapatkan dukungan dan akses ke sumber daya tambahan, bergabung dengan asosiasi atau lembaga keamanan siber seperti Asosiasi Keamanan Sistem (ISSA) atau Aliansi Keamanan Cloud (CSA).

SIMPULAN

Pentingnya peran pemerintah dalam membuat kebijakan keamanan siber dalam hal e-commerce Indonesia meningkatkan kepercayaan pengguna. Kesimpulan berikut mengenai peran pemerintah dalam hal ini: Perlindungan Pengguna: Untuk melindungi pengguna e-commerce, pemerintah membuat kebijakan dan undang-undang keamanan siber yang jelas. Tujuan kebijakan ini adalah untuk melindungi data pengguna dan menciptakan dasar hukum untuk memerangi kejahatan siber. Pembentukan Otoritas Keamanan Siber: Pemerintah Indonesia membentuk Badan Siber dan Sandi Negara (BSSN) dan otoritas keamanan siber lainnya untuk mengatur

upaya keamanan siber, memberikan pedoman, dan meningkatkan kemampuan keamanan secara keseluruhan. Kesadaran Publik: Pemerintah memiliki peran penting dalam meningkatkan kesadaran publik tentang bahaya dan cara melindungi diri dari keamanan siber. Kampanye pendidikan dan informasi dapat membantu pengguna lebih memahami keamanan siber. Kerjasama dengan Swasta: Pemerintah dapat mendorong kerjasama antara sektor swasta dan pemerintah untuk meningkatkan keamanan transaksi online. Ini dapat mencakup diskusi, pelatihan, dan bekerja sama untuk menetapkan standar keamanan.Regulasi Perlindungan Data: Regulasi yang mengatur perlindungan data pribadi harus dibuat dan diterapkan oleh pemerintah. Regulasi ini mengatur perusahaan e-commerce untuk melindungi dan memproses data pelanggan dengan aman. Respon Terhadap Insiden Keamanan: Pemerintah harus memiliki rencana yang efektif untuk menangani insiden keamanan. Ini termasuk berkolaborasi dengan lembaga penegak hukum, melakukan penyelidikan, dan mengambil tindakan cepat untuk mengatasi dan memberi tahu pengguna tentang pelanggaran keamanan. Kerjasama Internasional: Pemerintah dapat berpartisipasi dalam kerjasama internasional untuk mencegah ancaman siber internasional. Ini membantu dalam pertukaran data, pengenalan pelaku kejahatan siber, dan pengembangan praktik keamanan siber yang tersebar di seluruh dunia. Sanksi terhadap Pelanggaran: Hukum melarang pelanggaran keamanan siber dan menunjukkan keseriusan pemerintah dalam melindungi keamanan dan privasi pengguna e-commerce. Peraturan untuk Keamanan Infrastruktur Kritis: Infrastruktur penting yang mendukung e-commerce, seperti sistem logistik dan pembayaran, harus dilindungi oleh pemerintah. Infrastruktur harus dilindungi dengan standar keamanan yang ketat. Penyusunan Kebijakan Adaptif: Pemerintah harus membuat kebijakan keamanan siber yang fleksibel dan dapat diperbarui secara berkala karena ancaman siber terus berkembang. Dengan berpartisipasi secara proaktif dan komprehensif dalam membangun kebijakan ini, pemerintah dapat menciptakan lingkungan e-commerce yang lebih aman dan terpercaya, dan mendukung pertumbuhan ekonomi digital yang berkelanjutan di Indonesia. Ini akan

menumbuhkan kepercayaan pengguna, mendorong kreativitas, dan menciptakan lingkungan e-commerce yang sehat.

DAFTAR PUSTAKA

[1] L. Liu, M. K. O. Lee, R. Liu, and J. Chen, "Trust transfer in social media brand communities : The role of consumer engagement," *Elsevier*, vol. 41, no. 28, pp. 1–13, 2018, doi: 10.1016/j.ijinfomgt.2018.02.006.

[2] A. K. Kashyap and M. Chaudhary, "Cyber Security Laws And Safety In E-Commerce In India," *Law and Safety*, vol. 2, no. 1, pp. 207–218, 2023.

[3] J. Beckers, "COVID-19 and retail: The catalyst for e-commerce in Belgium?," *Journal of Retailing and Consumer Services*, vol. 62, 2021, doi: 10.1016/j.jretconser.2021.102645.

[4] H. S. Bella, "Pengaruh Persepsi Kebermanfaatan, Kepercayaan dan Computer Self Efficiency Terhadap Niatan Menggunakan e-Banking pada Mahasiswa," 2014.

[5] N. A. Muharam and A. Budianto, "Carding Crime Analysis as A Form of Cyber Crime in Indonesia ' s Criminal Law," *ICLSSEE*, vol. 1, no. 1, pp. 1–6, 2022, doi: 10.4108/eai.16-4-2022.2320085.

[6] Q. Atta and U. Haq, "Cyber Security and Analysis of Cyber-Crime Laws to Restrict Cyber Crime in Pakistan," *Computer Network and Information Security*, vol. 1, no. 1, pp. 62–69, 2019, doi: 10.5815/ijcnis.2019.01.06.

[7] S. O. Manullang, "The Legality of Devious Cyber Practices : Readiness of Indonesia ' s Cyber Laws," *Society*, vol. 10, no. 2, pp. 489–502, 2022, doi: 10.33019/society.v10i2.482.

[8] K. Ahmed, S. Khaldoon, and S. Hina, "Computers & Security CyberEntRel : Joint extraction of cyber entities and relations using deep learning," *Computers & Security*, vol. 136, no. August 2023, p. 103579, 2024, doi: 10.1016/j.cose.2023.103579.

[9] Z. P. A. Azzahra, Y. F. Furnamasari, and D. A. Dewi, "Pengaruh Teknologi Digital terhadap Persatuan dan Kesatuan Bangsa Indonesia," *Jurnal Pendidikan Tambusai*, vol. 5, no. 3, pp. 9232–9240, 2021.

[10] J. Da Silva, “Computers & Security Cyber security and the Leviathan,” *Computers & Security*, vol. 116, no. 1, p. 102674, 2022, doi: 10.1016/j.cose.2022.102674.

[11] Bambang Sutiyoso, “Penyelesaian Sengketa Bisnis Melalui Online Dipute Resolution dan Pemberlakuannya di Indonesia,” *Jurnal Mimbar Hukum*, vol. 20, no. Hukum Bisnis, pp. 230–240, 2004.

[12] B. D. Cone, C. E. Irvine, M. F. Thompson, and T. D. Nguyen, “A video game for cyber security training and awareness,” vol. 26, pp. 63–72, 2007, doi: 10.1016/j.cose.2006.10.005.

[13] S. Mamdouh, H. Bahsi, H. Ochieng, and T. Korõtko, “Computers & Security Threat Modeling of Cyber-Physical Systems - A Case Study of a Microgrid System,” *Computers & Security*, vol. 124, p. 102950, 2023, doi: 10.1016/j.cose.2022.102950.

[14] Ulya Amaliya, “E-Commerce in Singapore and Indonesia: A Policy Comparison,” *Jurnal Ilmu Sosial dan Ilmu Politik*, vol. 1, no. 2, pp. 1–21, 2009.

[15] Lia Catur Muliastuti, “Perlindungan Hukum Bagi Para Pihak Dalam Perjanjian Jual Beli Melalui Media Internet,” *Tesis Program Studi Magister Kenotariatan Program Pascasarjana Universitas Diponogoro*, pp. 1–133, 2010.

[16] I. M. Zaky Nur Husni, “Implementasi Business Intelligence Pada Manajemen Report Bank XYZ,” *Jurnal Sains Dan Senni Pomits*, vol. 3, no. 2, pp. 16–21, 2014.

[17] Bagus Hanindyo Mantri, “Legal Protection for Consumers in E-Commerce Transactions,” *Thesis for the Master of Law Program at Diponegoro University, Semarang*, pp. 1–88, 2007.

[18] X. Qin, F. Jiang, C. Dong, and R. Doss, “Computers & Security A hybrid cyber defense framework for reconnaissance attack in industrial control systems,” *Computers & Security*, vol. 136, no. July 2023, p. 103506, 2024, doi: 10.1016/j.cose.2023.103506.

[19] I. Fernandez, D. Arroyabe, C. F. A. Arranz, M. F. Arroyabe, J. Carlos, and F. De Arroyabe, “Computers & Security Cybersecurity capabilities and cyber-attacks as drivers of investment in cybersecurity systems : A UK survey for 2018 and

2019," *Computers & Security*, vol. 124, no. 1, p. 102954, 2023, doi: 10.1016/j.cose.2022.102954.

[20] R. Octora, P. L. S. Sewu, and J. A. Sugiono, "Regulation on electronic system security for E-wallet in order to protect consumers from financial loss due to cyber fraud based on Indonesian law," *… Journal of Social Science And Human …*. ijsshr.in, pp. 1–13, 2021. [Online]. Available: https://ijsshr.in/v4i9/Doc/1.pdf

[21] Mabizar, "Cyber security diplomacy and international Law.pdf." pp. 1–56, 2021.

[22] M. Lehto, "Strategic leadership in cyber security , case Finland," vol. 30, no. 3, pp. 139–148, 2021.

[23] B. Dupont, C. Shearing, M. Bernier, and R. Leukfeldt, "Computers & Security The tensions of cyber-resilience : From sensemaking to practice," vol. 132, 2023, doi: 10.1016/j.cose.2023.103372.

[24] Biuty Wulan Octavia, "Tinjauan Hukum Islam Terhadap Jual Beli Akad As-Salam Dengan Sistem Online Di Pand's Collection Pandanaran," *Skripsi Fakultas Syariah Institut Agama Islam Negeri Walisongo*, pp. 1–93, 2011.

[25] Debby Syarifah Anjaswari, "Analisis Implementasi Strategi Pemasaran di KJKS BMT Walisongo Semarang Dalam Perspektif Islam," *Skripsi*, no. Ekonomi dan Bisnis, pp. 1–70, 2015.

[26] Ali Murdiat, "Perlindungan Hukum Nasabah Penguna Ekektronik Banking Dalam Sistem Hukum Indonesia," *Jurnal Hukum*, vol. 1, no. Hukum ITE, pp. 57–70, 2013.

[27] Abdul Halim Barkatullah, ""'The Urgency of Protecting Consumer Rights in E-Commerce Transactions," *Jurnal Hukum*, vol. 2, no. 4, pp. 247–270, 2007.

[28] Ni Putu Ria Dewi Marhaeni, "Legal Protection for Consumers Relating to the Inclusion of Disclaimers by Business Actors on Internet Sites (Websites)," *Pascasarjana Universitas Udayana Denpasar*, pp. 1–196, 2013.

[29] P. R.A Marlien, "Pengaruh Reputasi, Privasi, dan Keamanan Terhadap Kepercayaan (Trust) Pengguna Internet di Semarang Dalam Sistem e-commerce," *Jurnal Manajemen dan Bisnis*, vol. 14, no. 2002, pp. 1–8, 2010.

[30] S. Veronika Asri Tanderirung, Riana T. Mangesa, "Pengenalan Cyber Security Bagi Siswa Sekolah Menengah Atas," *Pengabdian Masyarakat*, vol. 1, no. 2, pp. 89–94, 2023.

[31] B. P. Taufik Ramadhan, "Analysis of Information Security Awareness Level: Case Study of Digital Banking Application Users in Indonesia to Prevent Social Engineering," *Syntax Idea*, vol. 5, no. 1, pp. 86–97, 2023.

[32] Mikel Kelvin, "Pengaturan Kebebasan Berekspresi Melalui Media Digital Menurut Hukum Internasional dan Penerapannya Di Indoensia," *Skripsi Bagian Hukum internasional Fakultas Hukum Universitas Hasanudin Makasar*, pp. 1–118, 2016.

[33] I. Maria Utama, Iza Rumesten RS, "Digital Signature in E-Commerce Contract Disputes Based on Law no. 11 of 2008 concerning Electronic Information and Transactions," *Sriwijaya University Faculty of Law Scientific Magazine*, vol. 45, no. 2, pp. 2535–2549, 2008.

[34] Lis Febrianda, "Reconstruction of Regulations on Population Services and Civil Registration by Government Bureaucracy from the Perspective of State Administrative Law," *Dissertation of the Law Doctoral Program, Diponegoro University, Semarang*, pp. 1–400, 2009.

[35] Indra Tri Atmoko, "Sale and Purchase Agreement Through Online Shop Media Judging from Law no. 11 of 2008 concerning Information and Electronic Transactions," *Skripsi Fakultas Hukum Universitas Muhammadiyah Surakarta*, no. 11, pp. 1–21, 2013.

[36] V. R. Lailia, "Penerapan Strategi Pemasaran Digital Melalui Media Sosial Instagram Dalam Meningkatkan Penjualan Pada Arunazma," vol. 1, no. 2, 2023.

[37] Angga Christian, "Analisis Yuridis Sistem Transaksi Jual Beli Melalui Pihak Ketiga Secara Online Pada Situs Jual Beli Kaskus Dalam Website www.kaskus.co.id di Tinjau dari Prespektif Hukum Indonesia," *Skripsi Universitas Muhammadiyah Malang Fakultas Hukum*, pp. 1–12, 2016.

[38] B. S. Iwan Sidharta, "Pengaruh Kepuasan Transaksi Online Shooping dan Kepercayaan Konsumen Terhadap Sikap Serta Perilaku Konsumen Pada E-

Commerce," *Bisnis Jurnal Computech &*, vol. 9, no. 1, pp. 23–36, 2015.

[39] Elina Rudiastari, "Perlindungan Hukum Terhadap Konsumen Dalam Perjanjian Jual Beli Melalui e-Commerce di Indonesia," *Jurnal Sosial dan Humaniora*, vol. 5, no. Hukum Bisnis, pp. 71–81, 2015.

[40] Melisa Monica Sumenge, "Fraud Using Internet Media in the Form of Online Buying and Selling," *Jurnal Lex Crimen*, vol. 2, no. Hukum Bisnis, pp. 102–112, 2013.

[41] dkk Hasan Abdurahman, "Aplikasi Peminjaman Pembayaran Secara Kredit Pada Bank Yudha Bhakti," *Computech & Bisnis*, vol. 8, no. Aplikasi, pp. 61–69, 2014.

[42] A. Yaakop, Y. Shi, B. Foster, and ..., "Investigating e-wallet adoption of COVID19 intra-period among Malaysian youths': Integrated task-technology fit and technology acceptance model framework," *International Journal of ⋯*, 2021, [Online]. Available: http://m.growingscience.com/beta/ijds/4943-investigating-e-wallet-adoption-of-covid19-intra-period-among-malaysian-youths-integrated-task-technology-fit-and-technology-acceptance-model-framework.html

[43] S. Sumathi, S. N. Sivanandam, V. Lei, Z. Chen, and S. K. Nguang, *Introduction to Data Mining and its Applications Studies in Computational Intelligence , Volume 29 Further volumes of this series can be found on our homepage :*

[44] Saluky, "Aplikasi Business Intelligence Menggunakan Metode Balanced Scorecard untuk Mengukur Kinerja Marketing Indosat Cirebon," *Jurnal Informatika*, vol. 7, no. 2, pp. 191–200, 2011.

[45] Ardhata Nur Afian, "Pernjanjian Jual Beli Online," *Skripsi Fakultas Hukum Universitas Muhammadiyah Surakarta*, pp. 1–22, 2013.

[46] M. Khoiruman, "Model perlindungan hukum konsumen terhadap periklanan surat kabar (studi kasus surat kabar lokal di surakarta)," *Jurisprudence*, vol. 5, no. 2, pp. 34–43, 2015.

[47] D. Demitri Marvin Khadafi, "Perilaku Konsumen Dlam Memilih Jasa Layanan Operator Mobile Phone Yang Berbasis CDMA dan GSM," *Jurnal Wacana*, vol.

12, no. Perilaku Konsumen, pp. 216–231, 2009.

[48] Presiden Republik Indonesia, “Undang - Undang Republik Indonesia Nomor 8 Tahun 1999 Tentang Pelindungan Konsumen,” *Pemerintahan Indonesia*, pp. 1–46, 1999.

[49] N. Nur Fauziah and R. Wahyuningtyas, “Pengaruh Implementasi Inovasi Digital Terhadap Kinerja Perusahaan Berdasarkan Persepsi Karyawan (Studi Kasus Pada Pt. Indonesia Power Upjp Kamojang),” *Jurnal Mitra Manajemen*, vol. 4, no. 9, pp. 1378–1392, 2020, doi: 10.52160/ejmm.v4i9.462.

[50] Maria M. Ratna Sari, “Pengaruh Efektifitas Penggunaan dan Kepercayaan Terhadap Teknologi Sistem Informasi Akuntansi Terhadap Kinerja Individual Pada Pasar Swalayan di Kota Denpasar,” vol. 3, no. Ekonomi dan Akuntansi, pp. 1–21, 2012.