Jurnal Tana Mana
Vol. 4, No. 1, June 2023
https://ojs.staialfurqan.ac.id/jtm/

Perlindungan Data Pribadi terhadap Kebocoran Data Pelanggan *E-commerence* di Indonesia

Rachel Milafebina[1], Idham Putra Lesmana[2], Moody Rizqy Syailendra[3]
[1,2,3] *Universitas Tarumanagara Jakarta, Indonesia*

rachel.205220359@stu.untar.ac.id

Abstract

Protection of personal data is important in the digital world, especially in the E-Commerce business. In Indonesia, leaks of E-Commerce customer data are a frequent problem and are detrimental to consumers. Therefore, effective protection is needed to prevent customer data leakage. Leakage of customer data can occur due to various factors such as system errors, hacker attacks, and negligence of data managers. As a result, customer personal data such as telephone numbers, addresses and credit card information can be stolen and used for unsavory purposes. To solve this problem, the Indonesian government has issued a law on personal data protection. This law stipulates that any business that uses customer personal data must ensure the security of that data and protect consumers' privacy rights. This study aims to analyze the protection of personal data of e-commerce customers in Indonesia regarding data leakage. This study uses a qualitative approach by collecting data from literature and laws and regulations. The results of the study show that Indonesia has several civil law arrangements that protect the personal data of e-commerce customers. Regulations such as Law Number 11 of 2008 concerning Information and Electronic Transactions and Government Regulation Number 71 of 2019 concerning Implementation of Electronic Systems and Transactions regulate the obligations of e-commerce companies to protect customer personal data. To improve the protection of customers' personal data, cooperation between the government, industry players and the community is needed. The government needs to strengthen the implementation and enforcement of laws related to personal data protection. Industry players need to improve security and privacy systems, and involve certification bodies to ensure security standards are met. The public needs to increase awareness of the importance of protecting personal data and pay attention to the privacy policies set by e-commerce companies.

Keywords: Personal Data Protection, E-commerence Data Protection, Customer Data Leaks

Published by Fakultas Syariah Sekolah Tinggi Agama Islam (STAI) Al-Furqan Makassar
ISSN 2747-1667
Website https://ojs.staialfurqan.ac.id/jtm/

PENDAHULUAN

Perlindungan data pribadi merupakan salah satu aspek penting dalam penggunaan internet dan teknologi digital. Saat ini, semakin banyak perusahaan dan organisasi yang mengumpulkan, menyimpan, dan memproses data pribadi pelanggan mereka (Nugroho et al., 2020). Namun, risiko kebocoran data pelanggan juga semakin besar (Salim & Neltje, 2022). Dalam konteks *e-commerce*, kebocoran data pelanggan dapat terjadi akibat serangan siber atau tindakan tidak sah oleh pihak internal perusahaan. Oleh karena itu, diperlukan adanya perlindungan data pribadi yang kuat untuk melindungi pelanggan dari risiko kebocoran data.

Di Indonesia, perlindungan data pribadi diatur dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) (Gandhi et al., 2019). UU ITE ini bertujuan untuk mengatur penggunaan teknologi informasi dan elektronik, serta

memberikan perlindungan terhadap hak-hak pelanggan dalam transaksi elektronik. Salah satu hak pelanggan yang dilindungi dalam UU ITE adalah hak atas keamanan dan kerahasiaan data pribadi.

Selain UU ITE, perlindungan data pribadi juga diatur dalam Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik. Peraturan ini mengatur tentang pengumpulan, pengolahan, dan penggunaan data pribadi dalam sistem elektronik, serta tata cara pelaporan kebocoran data. Selain hukum perdata di Indonesia, terdapat juga kebijakan perlindungan data pribadi di tingkat internasional, yaitu General Data Protection Regulation (GDPR) yang berlaku di negara-negara Uni Eropa. Meskipun GDPR tidak langsung berlaku di Indonesia, namun perusahaan-perusahaan *e-commerce* yang beroperasi di Indonesia dan melakukan bisnis dengan negara-negara Uni Eropa harus mematuhi persyaratan GDPR.

Dalam konteks *e-commerce*, perusahaan *e-commerce* memiliki tanggung jawab untuk melindungi data pribadi pelanggan mereka (Setiawati et al., 2020). Perusahaan *e-commerce* harus mematuhi prinsip-prinsip perlindungan data pribadi, seperti pengumpulan data yang wajar dan proporsional, pengolahan data yang aman, serta penggunaan data hanya untuk tujuan yang sah (B & Wulandari, 2023). Perusahaan *e-commerce* juga harus menyediakan informasi yang jelas dan transparan mengenai penggunaan data pribadi pelanggan. Apabila terjadi kebocoran data pelanggan, perusahaan *e-commerce* harus segera memberitahu pelanggan mengenai kebocoran tersebut. Perusahaan *e-commerce* juga harus melakukan tindakan untuk mengurangi dampak kebocoran data, seperti mengambil tindakan keamanan yang lebih kuat dan menghentikan penggunaan data pribadi yang terdampak.

Selain itu, pelanggan juga memiliki hak untuk meminta akses, perbaikan, dan penghapusan data pribadi mereka dari perusahaan *e-commerce*. Apabila perusahaan *e-commerce* tidak mematuhi persyaratan perlindungan data pribadi, pelanggan dapat mengajukan gugatan ke pengadilan untuk meminta ganti rugi (Sulistiyono, 2022). Secara keseluruhan, perlindungan data pribadi menjadi semakin penting dalam era digital saat ini karena semakin banyaknya data pribadi yang dikumpulkan dan diproses oleh perusahaan dan organisasi (Anshori et al., 2022). Perusahaan dan organisasi mengumpulkan data pribadi pelanggan untuk berbagai kepentingan, seperti untuk memfasilitasi transaksi, meningkatkan layanan, dan melakukan analisis data. Namun, risiko kebocoran data pelanggan juga semakin besar, terutama karena semakin banyaknya serangan siber yang terjadi (Putri & Martha, 2021).

Kebocoran data pelanggan dapat menyebabkan kerugian yang signifikan bagi pelanggan, seperti pencurian identitas, penipuan keuangan, atau bahkan penggunaan data untuk kepentingan kriminal. Selain itu, kebocoran data pelanggan juga dapat merusak reputasi perusahaan atau organisasi yang mengumpulkan data tersebut, karena pelanggan akan kehilangan kepercayaan pada perusahaan atau organisasi tersebut. Oleh karena itu, perlindungan data pribadi menjadi semakin penting dalam era digital saat ini (Ratnasari et al., 2021). Negara-negara dan organisasi internasional telah mengeluarkan undang-undang dan regulasi untuk melindungi data pribadi pelanggan dari risiko kebocoran data. Selain itu, perusahaan dan organisasi juga harus mematuhi prinsip-prinsip perlindungan data pribadi, seperti pengumpulan data yang wajar dan proporsional, pengolahan data yang aman, serta penggunaan data hanya untuk tujuan yang sah.

Selain itu, pelanggan juga harus memperhatikan keamanan data pribadi mereka, seperti dengan menggunakan password yang kuat, tidak memberikan informasi pribadi kepada pihak yang tidak dikenal, dan memperbarui perangkat lunak keamanan secara teratur. Dalam konteks *e-commerce*, perlindungan data pribadi menjadi semakin penting karena *e-commerce* merupakan bisnis yang sangat bergantung pada data pribadi pelanggan (Hasibuan, 2022). Perusahaan *e-commerce* harus mematuhi persyaratan perlindungan data pribadi untuk memastikan bahwa data pribadi pelanggan mereka aman dari risiko kebocoran data (Sinaga et al., 2020).

Dalam era digital saat ini, perlindungan data pribadi menjadi tantangan yang semakin besar. Namun, dengan adanya undang-undang dan regulasi yang memadai, serta kesadaran yang lebih tinggi dari perusahaan, organisasi, dan pelanggan mengenai perlindungan data pribadi, diharapkan risiko kebocoran data pelanggan dapat ditekan dan perlindungan data pribadi dapat ditingkatkan.

METODE PENELITIAN

Penelitian mengenai perlindungan data pribadi terhadap kebocoran data pelanggan e-commerce di Indonesia merupakan topik yang penting untuk dibahas mengingat semakin maraknya penggunaan e-commerce di Indonesia serta meningkatnya kasus kebocoran data yang terjadi. Metode penelitian yang dapat digunakan untuk meneliti topik ini adalah studi literatur. Studi literatur adalah metode penelitian yang dilakukan dengan mengumpulkan dan menganalisis sumber informasi yang tersedia dalam bentuk tulisan atau literatur dari berbagai sumber seperti buku, jurnal, artikel, makalah, dan dokumen lainnya (Moleong, 2017). Metode ini dilakukan tanpa melakukan pengumpulan data secara langsung dari responden atau subjek penelitian. Studi literatur dapat dilakukan untuk mendapatkan informasi tentang topik tertentu, memperdalam pemahaman tentang teori, atau menemukan jawaban atas pertanyaan penelitian.

Langkah pertama dalam melakukan studi literatur adalah menentukan topik penelitian. Dalam hal ini, topik penelitian adalah perlindungan data pribadi terhadap kebocoran data pelanggan e-commerce di Indonesia. Setelah topik penelitian ditentukan, langkah selanjutnya adalah mencari sumber informasi yang relevan dengan topik tersebut. Sumber informasi dapat ditemukan melalui perpustakaan, internet, basis data jurnal, dan sumber lainnya. Setelah sumber informasi terkumpul, langkah selanjutnya adalah membaca dan mengevaluasi sumber informasi yang relevan. Evaluasi dilakukan untuk menentukan kualitas dan keakuratan informasi yang diperoleh dari sumber tersebut. Beberapa faktor yang perlu dievaluasi adalah reputasi sumber, metode penelitian yang digunakan, dan keakuratan data yang digunakan. Dalam melakukan evaluasi, peneliti perlu mempertimbangkan apakah sumber informasi yang ditemukan dapat mendukung jawaban dari pertanyaan penelitian yang telah ditetapkan sebelumnya. Setelah sumber informasi dievaluasi, langkah selanjutnya adalah mengekstrak informasi yang relevan dengan topik penelitian. Informasi yang relevan dapat ditemukan dalam bagian abstrak, pendahuluan, hasil penelitian, atau kesimpulan dari sumber informasi yang ditemukan. Setelah informasi ditemukan, peneliti perlu menyusun dan menganalisis informasi tersebut.

Dalam melakukan analisis, peneliti perlu mengorganisir informasi menjadi beberapa kategori atau tema. Kategori atau tema dapat dibuat berdasarkan sub-topik yang relevan dengan topik penelitian atau berdasarkan jenis data yang ditemukan. Setelah kategori atau tema dibuat, peneliti perlu menghubungkan dan membandingkan informasi yang ditemukan dalam setiap kategori atau tema. Hasil dari analisis studi literatur dapat digunakan untuk menemukan jawaban atas pertanyaan penelitian yang telah ditetapkan sebelumnya. Selain itu, hasil analisis dapat digunakan untuk mengidentifikasi kelemahan atau kekurangan penelitian yang telah dilakukan sebelumnya, memberikan saran atau rekomendasi untuk penelitian selanjutnya, dan memberikan kontribusi dalam pengembangan teori.

HASIL PENELITIAN DAN PEMBAHSAN

Pengaturan Hukum Perdata Terkait Perlindungan Data Pribadi Pelanggan *E-commerce*

E-commerce atau perdagangan elektronik saat ini telah menjadi salah satu bentuk perdagangan yang semakin populer di Indonesia (Rahmatullah, 2017). Penggunaan internet dan teknologi digital yang semakin meluas membuat kegiatan perdagangan elektronik semakin mudah dan nyaman. Namun, perkembangan perdagangan elektronik

juga membawa risiko terhadap keamanan dan privasi data pribadi pelanggan. Oleh karena itu, pemerintah Indonesia telah mengeluarkan beberapa peraturan dan undang-undang untuk melindungi data pribadi pelanggan e-commerce (Rohendi, 2015).

Pertama-tama, ada Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE) yang mengatur tentang perlindungan privasi dan keamanan data elektronik, termasuk data pribadi pelanggan e-commerce (Herryani, 2022). Pasal 26 ayat (1) UU ITE menegaskan bahwa setiap orang yang mengumpulkan, memproses, dan menyimpan data pribadi harus memastikan keamanan data tersebut. Pasal 28 ayat (1) UU ITE juga menyebutkan bahwa setiap orang yang memperoleh akses atas informasi elektronik atau dokumen elektronik yang berisi data pribadi harus menjaga kerahasiaan dan tidak menyebarluaskannya.

Kedua, ada Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik yang Menggunakan Sertifikat Elektronik. Peraturan ini mengatur tentang penyelenggaraan sistem dan transaksi elektronik yang menggunakan sertifikat elektronik. Pasal 29 ayat (1) huruf b Peraturan Pemerintah ini menegaskan bahwa penyelenggara harus melindungi data pribadi yang diperolehnya.

Selanjutnya, ada Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik. Peraturan ini mengatur tentang perlindungan data pribadi dalam sistem elektronik, termasuk dalam e-commerce. Pasal 6 Peraturan Menteri ini menegaskan bahwa setiap pemilik data pribadi berhak untuk mengetahui apa saja data pribadi yang dimilikinya, serta meminta perusahaan yang mengumpulkan data pribadi tersebut untuk mengubah atau menghapus data yang tidak akurat (Riyadi & Toto Tohir Suriaatmadja, 2023).

Selain itu, pada 2021, pemerintah Indonesia mengeluarkan Undang-Undang Nomor 11 Tahun 2021 tentang Cipta Kerja. UU ini mengatur tentang perlindungan data pribadi dalam rangka meningkatkan investasi dan daya saing Indonesia. Dalam UU ini, ada beberapa hal yang perlu diperhatikan terkait perlindungan data pribadi pelanggan e-commerce. Pertama, UU ini menetapkan bahwa setiap orang berhak atas perlindungan data pribadi yang diakui oleh hukum dan negara. Kedua, UU ini juga menetapkan bahwa setiap orang yang memproses data pribadi harus memastikan keamanan data tersebut. Ketiga, UU ini menetapkan bahwa setiap pemilik data pribadi berhak untuk mengetahui apa saja data pribadi yang dimilikinya dan bagaimana data tersebut digunakan (Ady et al., 2022).

Dalam praktiknya, meskipun sudah ada berbagai pengaturan hukum perdata terkait perlindungan data pribadi pelanggan e-commerce, masih banyak pelanggaran yang terjadi di lapangan. Pelanggaran ini dapat berupa pengumpulan data pribadi tanpa izin, penggunaan data pribadi secara tidak sah, penyebaran data pribadi tanpa persetujuan, atau bahkan kebocoran data pribadi karena tidak adanya tindakan keamanan yang memadai.

Oleh karena itu, penting bagi pemerintah dan pelaku e-commerce untuk meningkatkan kesadaran dan pemahaman tentang pentingnya perlindungan data pribadi. Selain itu, diperlukan juga penegakan hukum yang tegas terhadap pelanggaran yang dilakukan oleh pelaku e-commerce. Pemerintah perlu meningkatkan pengawasan dan pengendalian terhadap pengumpulan, pengolahan, dan penggunaan data pribadi pelanggan e-commerce. Penting juga bagi pelaku e-commerce untuk mengembangkan kebijakan dan praktik terbaik dalam pengumpulan dan pengolahan data pribadi pelanggan. Hal ini dapat dilakukan melalui pengembangan kebijakan privasi dan pengamanan data yang jelas dan transparan. Pelaku e-commerce juga harus memberikan informasi yang jelas dan mudah dipahami kepada pelanggan mengenai pengumpulan dan penggunaan data pribadi mereka.

Selain itu, pelanggan juga dapat berperan aktif dalam melindungi data pribadi mereka. Pelanggan harus berhati-hati dalam memberikan informasi pribadi pada saat melakukan transaksi online. Pelanggan juga harus memeriksa kebijakan privasi dan keamanan data yang disediakan oleh pelaku e-commerce sebelum melakukan transaksi. Pengaturan hukum perdata terkait perlindungan data pribadi pelanggan *e-commerce* di Indonesia sudah cukup

baik. Namun, masih diperlukan upaya untuk meningkatkan kesadaran dan pemahaman masyarakat mengenai pentingnya perlindungan data pribadi. Pemerintah dan pelaku *e-commerce* juga harus melakukan tindakan yang tegas terhadap pelanggaran yang dilakukan oleh pelaku *e-commerce*. Semua pihak harus bekerja sama untuk memastikan bahwa *e-commerce* dapat memberikan manfaat bagi masyarakat dengan tetap menjaga keamanan dan privasi data pribadi pelanggan.

Studi Kasus

Salah satu studi kasus perlindungan data pribadi terhadap kebocoran data pelanggan *e-commerce* di Indonesia adalah insiden kebocoran data yang melibatkan perusahaan *e-commerce* Bukalapak pada tahun 2020. Berikut adalah deskripsi studi kasus tersebut:

1. Kejadian: Pada November 2020, Bukalapak mengumumkan bahwa mereka telah mengalami kebocoran data yang melibatkan informasi pribadi sekitar 13 juta pengguna. Data yang bocor termasuk nama lengkap, alamat email, nomor telepon, alamat pengiriman, serta beberapa informasi terkait transaksi.
2. Penyebab Kebocoran Data: Bukalapak menyatakan bahwa kebocoran data terjadi akibat serangan siber yang mengarah pada eksploitasi celah keamanan di sistem mereka. Penyerang berhasil mengakses server Bukalapak dan mencuri data pengguna.
3. Dampak: Kebocoran data ini mengakibatkan potensi risiko bagi privasi dan keamanan pengguna Bukalapak. Informasi pribadi yang dicuri dapat digunakan untuk aktivitas penipuan, spam, atau serangan siber lainnya. Selain itu, insiden ini juga merusak kepercayaan pengguna terhadap Bukalapak dan meningkatkan kekhawatiran tentang perlindungan data dalam industri *e-commerce*.
4. Respons dan Tindakan: Setelah mengungkapkan kebocoran data, Bukalapak segera mengambil langkah-langkah untuk mengatasi situasi ini. Mereka secara aktif berkoordinasi dengan otoritas terkait, termasuk Komisi Pemberantasan Korupsi (KPK) dan Badan Siber dan Sandi Negara (BSSN), untuk menyelidiki kejadian ini. Bukalapak juga memberikan pemberitahuan resmi kepada pengguna terdampak dan memberikan panduan tentang langkah-langkah yang dapat diambil untuk melindungi diri.
5. Peningkatan Keamanan dan Kebijakan: Setelah kejadian ini, Bukalapak meningkatkan langkah-langkah keamanan mereka dengan memperkuat sistem dan infrastruktur mereka, serta melibatkan penyedia layanan keamanan siber untuk melakukan audit dan pengujian keamanan. Mereka juga meningkatkan kesadaran internal dan pelatihan karyawan tentang keamanan data.
6. Pelajaran yang Dipetik: Studi kasus ini menggarisbawahi pentingnya perlindungan data pribadi dalam industri e-commerce. Perusahaan-perusahaan e-commerce harus memastikan keamanan sistem mereka dan mengadopsi langkah-langkah proaktif untuk melindungi data pelanggan. Penyusunan kebijakan privasi yang jelas, pemantauan keamanan yang terus-menerus, dan peningkatan kesadaran tentang keamanan siber menjadi faktor penting dalam mencegah dan merespons kebocoran data.

Kebocoran data pelanggan merupakan ancaman serius bagi privasi dan keamanan konsumen. Studi kasus Bukalapak ini menunjukkan pentingnya upaya perlindungan data pribadi yang kuat dalam industri e-commerce dan perlunya perusahaan *e-commerce* untuk mengambil tindakan proaktif untuk mencegah serangan dan mengatasi kebocoran data dengan cepat.

Pengaruh Kebocoran Data Pelanggan Terhadap Hak-Hak Perdata Pelanggan *E-commerce*

E-commerce telah menjadi bagian penting dari kehidupan kita di era digital saat ini. Banyak pelanggan yang melakukan transaksi online untuk membeli produk dan jasa (Indriyani, 2017). Namun, sebagai pengguna *e-commerce*, kita harus mengerti bahwa setiap kali kita melakukan transaksi online, kita memberikan informasi pribadi kepada pelaku *e-commerce*, seperti nama, alamat, nomor telepon, dan bahkan nomor kartu kredit. Kebocoran data pelanggan dapat terjadi dan dapat mengancam hak-hak perdata pelanggan *e-commerce* di Indonesia (Sonjaya & Setiawan, 2022).

Kebocoran data pelanggan *e-commerce* dapat terjadi karena berbagai alasan, seperti kelalaian dalam pengolahan data, serangan siber oleh hacker, atau kebocoran oleh pihak internal. Kebocoran data ini dapat mengakibatkan kerugian yang signifikan bagi pelanggan e-commerce. Hal ini dapat merusak citra dan reputasi pelanggan, serta menimbulkan kerugian finansial dan emosional. Lebih dari itu, kebocoran data pelanggan dapat mengancam hak-hak perdata pelanggan *e-commerce* di Indonesia.

Salah satu hak perdata pelanggan *e-commerce* adalah hak atas privasi. Kebocoran data dapat mengancam hak privasi pelanggan. Informasi pribadi seperti nama, alamat, dan nomor telepon dapat digunakan untuk melakukan penipuan, pengiriman spam, dan serangan phishing. Selain itu, kebocoran nomor kartu kredit dapat digunakan oleh orang yang tidak bertanggung jawab untuk melakukan penipuan atau pembelian yang tidak sah. Hal ini dapat merugikan pelanggan secara finansial dan emosional.

Selain hak atas privasi, pelanggan *e-commerce* juga memiliki hak atas perlindungan data pribadi. Kebocoran data pelanggan dapat mengancam hak perlindungan data pribadi pelanggan *e-commerce* (Muhammad & Nugroho, 2021). Data pelanggan yang dicuri dapat digunakan untuk kepentingan komersial atau kriminal. Data pelanggan dapat dijual ke pihak ketiga atau digunakan untuk melakukan penipuan identitas. Hal ini dapat mengancam keamanan dan privasi data pribadi pelanggan e-commerce, serta dapat menyebabkan kerugian finansial dan emosional.

Selain hak atas privasi dan hak atas perlindungan data pribadi, pelanggan *e-commerce* juga memiliki hak atas pengaduan dan kompensasi. Kebocoran data pelanggan dapat mengancam hak pelanggan untuk mengajukan pengaduan dan mendapatkan kompensasi. Jika terjadi kebocoran data, pelanggan dapat mengajukan pengaduan kepada pelaku *e-commerce* dan meminta kompensasi atas kerugian yang diderita. Namun, jika pelaku *e-commerce* tidak merespons dengan baik, pelanggan dapat kehilangan hak mereka untuk mengajukan pengaduan dan mendapatkan kompensasi. Kebocoran data pelanggan *e-commerce* juga dapat mengancam hak pelanggan untuk mengontrol data pribadi mereka. Pelanggan *e-commerce* memiliki hak untuk mengontrol data pribadi mereka dan menentukan bagaimana data tersebut digunakan. Namun, jika terjadi kebocoran data, pelanggan kehilangan kendali atas data pribadi mereka dan tidak dapat memastikan bagaimana data tersebut digunakan (Harahap et al., 2023).

Kebocoran data pelanggan e-commerce dapat juga mengancam hak pelanggan untuk mendapatkan akses ke informasi tentang pengumpulan dan penggunaan data pribadi mereka. Pelanggan *e-commerce* berhak untuk mengetahui bagaimana data pribadi mereka dikumpulkan dan digunakan oleh pelaku *e-commerce*. Namun, jika terjadi kebocoran data, pelanggan tidak dapat memastikan bagaimana data pribadi mereka dikumpulkan dan digunakan oleh pelaku *e-commerce*. Hal ini dapat mengancam hak pelanggan untuk mendapatkan akses ke informasi tentang pengumpulan dan penggunaan data pribadi mereka.

Kebocoran data pelanggan *e-commerce* juga dapat mengancam hak pelanggan untuk meminta penghapusan data pribadi mereka. Pelanggan *e-commerce* memiliki hak untuk meminta penghapusan data pribadi mereka jika data tersebut tidak lagi diperlukan oleh pelaku *e-commerce* atau jika pengolahan data tersebut melanggar undang-undang. Namun,

jika terjadi kebocoran data, pelanggan tidak dapat memastikan apakah data pribadi mereka sudah dihapus atau tidak. Dalam menghadapi kebocoran data pelanggan *e-commerce*, pelanggan dapat mengambil langkah-langkah untuk melindungi hak-hak perdata mereka. Pertama, pelanggan dapat memastikan bahwa mereka hanya memberikan informasi pribadi yang diperlukan saat melakukan transaksi online. Kedua, pelanggan dapat memastikan bahwa mereka hanya melakukan transaksi dengan pelaku e-commerce yang terpercaya dan telah menerapkan sistem keamanan yang baik. Ketiga, pelanggan dapat memantau aktivitas transaksi mereka dan memeriksa laporan tagihan kartu kredit mereka secara teratur untuk mendeteksi aktivitas yang mencurigakan.

Sementara itu, pemerintah dan regulator juga berperan penting dalam melindungi hak-hak perdata pelanggan *e-commerce* di Indonesia. Pemerintah dapat mengembangkan undang-undang yang lebih ketat terkait perlindungan data pribadi pelanggan *e-commerce*. Regulator dapat memantau dan menegakkan kepatuhan pelaku e-commerce terhadap undang-undang perlindungan data pribadi dan menerapkan sanksi yang tegas bagi pelaku *e-commerce* yang melanggar aturan. Kebocoran data pelanggan *e-commerce* dapat mengancam hak-hak perdata pelanggan *e-commerce* di Indonesia. Kebocoran data dapat mengancam hak atas privasi, hak atas perlindungan data pribadi, hak atas pengaduan dan kompensasi, hak untuk mengontrol data pribadi, hak untuk mendapatkan akses ke informasi tentang pengumpulan dan penggunaan data pribadi, dan hak untuk meminta penghapusan data pribadi. Oleh karena itu, pelanggan dan pemerintah harus bekerja sama untuk melindungi hak-hak perdata pelanggan e-commerce di Indonesia dan mencegah kebocoran data yang dapat mengancam hak-hak perdata tersebut.

Mekanisme Penyelesaian Sengketa Perdata Terkait Kebocoran Data Pelanggan

Penyelesaian sengketa perdata terkait kebocoran data pelanggan di Indonesia dapat dilakukan melalui beberapa mekanisme, seperti perundingan, mediasi, arbitrase, atau melalui jalur litigasi di pengadilan (Fathur, 2020). Setiap mekanisme memiliki kelebihan dan kelemahan masing-masing, sehingga para pihak harus mempertimbangkan faktor-faktor tersebut dalam memilih mekanisme yang tepat untuk menyelesaikan sengketa mereka (Edu, 2022).

1. Perundingan

   Perundingan merupakan salah satu mekanisme penyelesaian sengketa yang paling umum digunakan. Dalam perundingan, para pihak yang terlibat dalam sengketa berusaha untuk mencapai kesepakatan melalui diskusi dan negosiasi. Perundingan dapat dilakukan secara langsung antara para pihak atau melalui perantara yang bersifat netral, seperti mediator atau pengacara. Keuntungan dari perundingan adalah bahwa para pihak dapat mencapai kesepakatan secara cepat dan murah. Selain itu, perundingan juga dapat menciptakan hubungan yang baik antara para pihak setelah sengketa diselesaikan. Namun, perundingan juga memiliki kelemahan, seperti ketidakpastian dan kekurangan alat pemaksaan jika salah satu pihak tidak memenuhi kesepakatan yang telah dicapai.

2. Mediasi

   Mediasi merupakan mekanisme penyelesaian sengketa di mana mediator membantu para pihak untuk mencapai kesepakatan melalui diskusi dan negosiasi. Mediator biasanya memiliki keterampilan dalam membantu para pihak untuk memahami masalah dan menemukan solusi yang menguntungkan semua pihak. Keuntungan dari mediasi adalah bahwa para pihak dapat mencapai kesepakatan yang memuaskan tanpa harus melalui jalur litigasi yang panjang dan mahal. Selain itu, mediasi juga dapat membantu menjaga hubungan yang baik antara para pihak setelah sengketa diselesaikan. Namun, mediasi juga memiliki kelemahan, seperti ketidakpastian dan kekurangan alat pemaksaan jika salah satu pihak tidak memenuhi kesepakatan yang telah dicapai.

3. Arbitrase

   Arbitrase merupakan mekanisme penyelesaian sengketa di mana para pihak menyepakati untuk menyelesaikan sengketa mereka melalui arbitrator yang bersifat netral. Arbitrator akan memutuskan sengketa tersebut dan keputusan tersebut bersifat final dan mengikat.

   Keuntungan dari arbitrase adalah bahwa para pihak dapat menyelesaikan sengketa mereka secara cepat dan efisien. Selain itu, arbitrase juga bersifat privat dan dapat dilakukan dengan rahasia, sehingga dapat menghindari publisitas yang tidak diinginkan. Namun, arbitrase juga memiliki kelemahan, seperti biaya yang tinggi dan kekurangan mekanisme banding jika salah satu pihak tidak puas dengan keputusan yang telah diambil.

4. Litigasi

   Litigasi merupakan mekanisme penyelesaian sengketa di mana para pihak menyelesaikan sengketa mereka melalui pengadilan. Litigasi memungkinkan para pihak untuk memperoleh keputusan yang bersifat final dan mengikat melalui proses pengadilan yang formal dan terstruktur. Keuntungan dari litigasi adalah bahwa para pihak dapat memperoleh keputusan yang bersifat final dan mengikat melalui proses pengadilan yang formal dan terstruktur. Selain itu, litigasi juga memungkinkan para pihak untuk memperoleh ganti rugi yang memadai jika terdapat kerugian yang ditimbulkan. Namun, litigasi juga memiliki kelemahan, seperti biaya yang tinggi, waktu yang lama, dan publisitas yang tidak diinginkan.

Dalam konteks kebocoran data pelanggan, mekanisme penyelesaian sengketa yang paling sesuai tergantung pada karakteristik sengketa yang terjadi. Jika sengketa tersebut melibatkan kerugian yang relatif kecil dan para pihak masih mempertahankan hubungan yang baik, maka perundingan atau mediasi mungkin merupakan mekanisme yang paling tepat. Namun, jika sengketa tersebut melibatkan kerugian yang besar atau terdapat perselisihan yang kuat antara para pihak, maka arbitrase atau litigasi mungkin merupakan mekanisme yang lebih tepat.

Dalam kasus kebocoran data pelanggan, mekanisme penyelesaian sengketa yang paling sesuai adalah melalui litigasi di pengadilan (Satrio & Widiatno, 2020). Hal ini karena kebocoran data pelanggan dapat menimbulkan kerugian yang signifikan bagi para pelanggan e-commerce, dan para pelanggan memiliki hak untuk memperoleh ganti rugi yang memadai (Sylfia et al., 2021). Selain itu, litigasi juga memungkinkan para pelanggan untuk mengajukan tuntutan pidana jika terdapat tindakan penyalahgunaan data yang melanggar hukum. Namun, sebelum mengambil jalur litigasi, para pelanggan dapat mencoba untuk menyelesaikan sengketa melalui perundingan atau mediasi terlebih dahulu. Jika sengketa tersebut tidak dapat diselesaikan melalui jalur ini, maka para pelanggan dapat mengajukan tuntutan melalui pengadilan. Proses litigasi dapat memakan waktu dan biaya yang signifikan, namun para pelanggan dapat memperoleh ganti rugi yang memadai jika terdapat kerugian yang ditimbulkan oleh kebocoran data pelanggan.

Dalam penyelesaian sengketa perdata terkait kebocoran data pelanggan, penting untuk mempertimbangkan faktor-faktor seperti biaya, waktu, dan kerumitan proses. Selain itu, para pelanggan juga perlu memastikan bahwa mereka bekerja sama dengan pengacara yang kompeten dan berpengalaman dalam penyelesaian sengketa perdata terkait kebocoran data pelanggan. Dengan cara ini, para pelanggan dapat memperoleh perlindungan hukum yang memadai dan memastikan bahwa hak-hak mereka diakui dan dilindungi secara efektif.

Tanggung Jawab Perusahaan Dalam Menjaga Keamanan Data Pribadi Pelanggan

Perusahaan *e-commerce* memiliki tanggung jawab yang besar dalam menjaga keamanan data pribadi pelanggan, terutama karena data pribadi tersebut dapat digunakan untuk tujuan yang tidak diinginkan jika jatuh ke tangan yang salah (van Ooijen & Vrabec,

2019). Oleh karena itu, di Indonesia terdapat beberapa peraturan hukum yang mengatur tentang perlindungan data pribadi pelanggan e-commerce, seperti UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dan Peraturan Pemerintah No. 71 Tahun 2019 tentang Pelaksanaan UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Benuf et al., 2019).

Tanggung jawab perusahaan e-commerce dalam menjaga keamanan data pribadi pelanggan diatur oleh peraturan hukum tersebut (Lobschat et al., 2021). Perusahaan e-commerce harus memastikan bahwa data pribadi pelanggan yang mereka miliki tidak disalahgunakan atau disalahgunakan oleh pihak lain (Rahmi Ayunda, 2021). Tanggung jawab tersebut mencakup:

1. Menjaga kerahasiaan data pribadi pelanggan Perusahaan e-commerce harus menjaga kerahasiaan data pribadi pelanggan dan tidak mengungkapkannya kepada pihak lain tanpa izin dari pelanggan atau kepentingan hukum yang sah. Hal ini termasuk melindungi data pribadi pelanggan dari akses yang tidak sah dan melindungi data pribadi tersebut dari risiko kebocoran.
2. Melindungi data pribadi pelanggan dari risiko kebocoran Perusahaan e-commerce harus memastikan bahwa sistem keamanan mereka memadai untuk melindungi data pribadi pelanggan dari risiko kebocoran. Ini mencakup mengadopsi kebijakan dan prosedur keamanan yang ketat, seperti enkripsi data, autentikasi pengguna, dan pengawasan akses.
3. Memberikan informasi yang jelas tentang penggunaan data pribadi pelanggan Perusahaan e-commerce harus memberikan informasi yang jelas dan transparan tentang penggunaan data pribadi pelanggan, termasuk tentang pengumpulan data, tujuan pengumpulan data, dan pihak yang memiliki akses ke data tersebut. Perusahaan e-commerce juga harus memperoleh izin dari pelanggan sebelum menggunakan data pribadi mereka untuk tujuan tertentu.
4. Memberikan akses dan kontrol yang memadai bagi pelanggan atas data pribadi mereka Perusahaan e-commerce harus memberikan akses dan kontrol yang memadai kepada pelanggan atas data pribadi mereka, seperti memungkinkan pelanggan untuk memperbarui, memperbaiki, atau menghapus data pribadi mereka dari sistem perusahaan.

Untuk memenuhi kewajiban mereka dalam menjaga keamanan data pribadi pelanggan, perusahaan e-commerce harus mengadopsi kebijakan dan prosedur keamanan yang memadai, serta memastikan bahwa karyawan mereka memahami dan mematuhi kebijakan tersebut (Delpiero et al., 2021). Beberapa cara yang dapat dilakukan oleh perusahaan e-commerce untuk memenuhi kewajiban mereka dalam menjaga keamanan data pribadi pelanggan adalah sebagai berikut:

1. Memperbarui kebijakan privasi dan penggunaan data Perusahaan e-commerce harus teratur untuk mencerminkan perubahan dalam kebutuhan keamanan dan privasi, serta untuk memastikan kesesuaian dengan peraturan hukum yang berlaku.
2. Mengadopsi teknologi keamanan yang memadai Perusahaan e-commerce harus mengadopsi teknologi keamanan yang memadai, seperti firewalls, enkripsi data, autentikasi pengguna, dan pengawasan akses. Selain itu, mereka juga harus memastikan bahwa teknologi tersebut dijaga dengan baik dan diperbarui secara teratur.
3. Melatih karyawan mengenai keamanan data Perusahaan e-commerce harus melatih karyawan mereka mengenai keamanan data dan privasi, termasuk pentingnya menjaga kerahasiaan data pribadi pelanggan, cara mengelola data dengan aman, dan cara mengenali potensi ancaman keamanan.
4. Memantau dan melaporkan potensi pelanggaran keamanan data Perusahaan e-commerce harus memantau aktivitas penggunaan data mereka secara teratur untuk mendeteksi potensi ancaman keamanan dan memastikan bahwa kebijakan keamanan

dan privasi mereka diterapkan dengan benar. Jika terjadi pelanggaran keamanan data, mereka juga harus melaporkannya kepada pelanggan dan otoritas yang berwenang sesuai dengan peraturan hukum yang berlaku.

5. Menyediakan pusat bantuan untuk pelanggan Perusahaan e-commerce harus menyediakan pusat bantuan untuk pelanggan mereka, di mana pelanggan dapat memperoleh informasi tentang kebijakan privasi dan penggunaan data perusahaan, serta memperbarui, memperbaiki, atau menghapus data pribadi mereka dari sistem perusahaan.

Dalam rangka memenuhi kewajiban mereka dalam menjaga keamanan data pribadi pelanggan, perusahaan e-commerce juga harus memastikan bahwa mereka memiliki sumber daya dan dana yang cukup untuk mengelola dan melindungi data pribadi pelanggan dengan baik. Selain itu, mereka harus memperbarui kebijakan dan prosedur keamanan mereka secara teratur untuk mencerminkan perubahan dalam kebutuhan keamanan dan privasi, serta untuk memastikan kesesuaian dengan peraturan hukum yang berlaku. Perusahaan e-commerce memiliki tanggung jawab yang besar dalam menjaga keamanan data pribadi pelanggan mereka, dan harus memastikan bahwa mereka memenuhi kewajiban mereka sesuai dengan peraturan hukum yang berlaku. Melalui pengadopsian kebijakan dan prosedur keamanan yang memadai, serta melatih karyawan dan menyediakan pusat bantuan untuk pelanggan, perusahaan e-commerce dapat memastikan bahwa data pribadi pelanggan mereka aman dan terlindungi dari risiko kebocoran.

Upaya Pemerintah dan Pelaku Industri Dalam Meningkatkan Kesadaran dan Perlindungan Data Pribadi Pelanggan

Pemerintah dan pelaku industri di Indonesia telah melakukan beberapa upaya untuk meningkatkan kesadaran dan perlindungan data pribadi pelanggan di Indonesia (Disemadi, 2021). Berikut adalah beberapa upaya yang dilakukan:

1. Regulasi dan peraturan hukum Pemerintah Indonesia telah mengeluarkan beberapa peraturan hukum untuk meningkatkan perlindungan data pribadi, seperti UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, PP No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, dan PP No. 82 Tahun 2012 tentang Perlindungan Data Pribadi. Hal ini memastikan bahwa perusahaan wajib menjaga kerahasiaan data pribadi pelanggan dan memberikan perlindungan terhadap penggunaan data pribadi yang tidak sah.
2. Penegakan hukum Pemerintah dan lembaga penegak hukum telah melakukan tindakan hukum terhadap pelanggaran privasi dan keamanan data, seperti memberikan sanksi kepada perusahaan yang melanggar aturan perlindungan data pribadi. Ini termasuk sanksi administratif, seperti denda atau pembatasan operasional, dan sanksi pidana, seperti penjara atau denda yang lebih besar.
3. Kampanye Kesadaran Publik Pemerintah dan pelaku industri telah meluncurkan kampanye kesadaran publik tentang perlindungan data pribadi untuk meningkatkan kesadaran masyarakat mengenai pentingnya privasi dan keamanan data pribadi. Kampanye tersebut dilakukan dengan berbagai cara, seperti seminar, workshop, dan pelatihan di berbagai tempat, termasuk sekolah dan universitas.
4. Sertifikasi dan Akreditasi Ada beberapa lembaga sertifikasi dan akreditasi yang menawarkan sertifikasi keamanan data pribadi untuk membantu perusahaan meningkatkan kualitas dan standar keamanan mereka. Sertifikasi ini membantu perusahaan memastikan bahwa mereka memenuhi standar tertentu untuk menjaga privasi dan keamanan data pribadi pelanggan mereka.
5. Kerja sama internasional Pemerintah Indonesia telah melakukan kerja sama internasional untuk meningkatkan kesadaran dan perlindungan data pribadi, seperti bekerja sama dengan negara-negara lain dalam menyusun standar keamanan data dan mengatasi pelanggaran privasi dan keamanan data. Kerja sama ini membantu

Indonesia untuk mempelajari praktik terbaik dari negara-negara lain dan mengadopsi mereka sesuai dengan kondisi lokal.

Dalam rangka meningkatkan kesadaran dan perlindungan data pribadi pelanggan, penting bagi pemerintah dan pelaku industri untuk terus melakukan upaya-upaya tersebut (Dharu Triasih, Dewi Tuti Muryati, 2021). Pemerintah perlu terus memperbarui regulasi dan peraturan hukum yang berkaitan dengan perlindungan data pribadi, sementara pelaku industri harus terus meningkatkan sistem keamanan dan privasi mereka. Selain itu, penting juga untuk melibatkan masyarakat dan meningkatkan kesadaran mereka melalui kampanye kesadaran publik dan pelatihan. Dengan melakukan hal ini, Indonesia dapat memastikan bahwa data pribadi pelanggan dijaga dan dilindungi dengan baik.

KESIMPULAN

Kebocoran data pribadi pelanggan *e-commerce* di Indonesia merupakan masalah serius yang dapat mempengaruhi hak-hak perdata pelanggan, seperti hak atas privasi dan keamanan data. Untuk itu, pemerintah Indonesia telah mengeluarkan beberapa regulasi dan peraturan hukum untuk meningkatkan perlindungan data pribadi pelanggan *e-commerce*. Selain itu, pelaku industri di Indonesia juga harus bertanggung jawab dalam menjaga keamanan data pribadi pelanggan dan memenuhi kewajiban mereka dalam hal ini. Upaya-upaya yang dilakukan antara lain meningkatkan sistem keamanan dan privasi, memberikan pelatihan kepada karyawan tentang perlindungan data pribadi, serta melibatkan lembaga sertifikasi dan akreditasi untuk memastikan bahwa standar keamanan dan privasi terpenuhi. Tidak hanya pemerintah dan pelaku industri, tetapi kesadaran masyarakat juga menjadi faktor penting dalam perlindungan data pribadi pelanggan *e-commerce* di Indonesia. Kampanye kesadaran publik dan pelatihan harus terus dilakukan agar masyarakat dapat memahami pentingnya privasi dan keamanan data pribadi mereka serta melakukan tindakan pencegahan yang tepat. Secara keseluruhan, perlindungan data pribadi pelanggan *e-commerce* di Indonesia masih perlu terus ditingkatkan melalui upaya bersama dari pemerintah, pelaku industri, dan masyarakat. Dengan menjaga privasi dan keamanan data pribadi, diharapkan dapat menciptakan lingkungan *e-commerce* yang aman dan dapat dipercaya bagi pelanggan.

REFERENSI

Ady, E. N. S., Nisrina, F. B., Ramadhani, F., & Irawan, F. (2022). Urgensi KUHD Dalam Menangani Risiko Kejahatan Siber Pada Transaksi E-Commerce. *Journal of Law, Administration, and Social Science*, *2*(1), 45–55. https://doi.org/10.54957/jolas.v2i1.166

Anshori, M. Y., Karya, D. F., & Gita, M. N. (2022). Study on the Reuse Intention of E-Commerce Platform Applications: Security, Privacy, Perceived Value, and Trust. *Jurnal Manajemen Teori Dan Terapan | Journal of Theory and Applied Management*, *15*(1), 13–24. https://doi.org/10.20473/jmtt.v15i1.34923

B, S. D., & Wulandari, S. (2023). *Telecommunication Company Against Consumer Personal Information Data Leakage*. Atlantis Press SARL. https://doi.org/10.2991/978-2-38476-024-4

Benuf, K., Mahmudah, S., & Priyono, E. A. (2019). Perlindungan Hukum Terhadap Keamanan Data Konsumen Financial Technology Di Indonesia. *Refleksi Hukum: Jurnal Ilmu Hukum*, *3*(2), 145–160. https://doi.org/10.24246/jrh.2019.v3.i2.p145-160

Delpiero, M., Reynaldi, F. A., Ningdiah, I. U., & Muthmainnah, N. (2021). Analisis Yuridis Kebijakan Privasi dan Pertanggungjawaban Online Marketplace Dalam Perlindungan Data Pribadi Pengguna Pada Kasus Kebocoran Data. *Padjadjaran Law*, *9*(1), 1–22.

Dharu Triasih, Dewi Tuti Muryati, A. H. N. (2021). Perlindungan Hukum Bagi Konsumen Dalam Perjanjian Pinjaman Online. *Digilib.Uin-Suka.Ac.Id*, *7*(2), 591–608.

Disemadi, H. S. (2021). Fenomena Predatory Lending: Suatu Kajian Penyelenggaraan Bisnis Fintech P2P Lending selama Pandemi COVID-19 di Indonesia. *Pandecta Research Law Journal*, *16*(1), 55–67.

Edu, H. (2022). Perlindungan Hukum atas Kebocoran Data Pribadi Konsumen pada E-Commerce. *Heylaw.Edu*, *3*(1), 143–148.

Fathur, M. (2020). Tanggung Jawab Tokopedia Terhadap Kebocoran Data. *National Conference on Law Studies (NCOLS)*, *2*(1), 43–60.

Gandhi, A., Sucahyo, Y. G., & Ruldeviyani, Y. (2019). Investigating the protection of customers' personal data in the ridesharing applications: A desk research in Indonesia. *ECTI-CON 2018 - 15th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology*, *1*, 118–121. https://doi.org/10.1109/ECTICon.2018.8619912

Harahap, W. F., Daulay, A. R. R., Alfisyahri, P. N., & Silalahi, P. R. (2023). Analisis Citra Market Place Pt Tokopedia Dalam Meningkatkan Kepercayaan Konsumen Pasca Kebocoran Data Pengguna. *CEMERLANG : Jurnal Manajemen Dan Ekonomi Bisnis*, *3*(1), 29–41.

Hasibuan, E. (2022). *Legal Protection of Consumer Personal Data in E-Commerce Transactions During the Covid-19 Pandemic*. https://doi.org/10.4108/eai.8-6-2021.2314335

Herryani, M. (2022). Perlindungan Hukum Terhadap Kebocoran Data Pribadi Konsumen Online Marketace. *Transparansi Hukum*, *5*(1), 110–133.

Indriyani, M. (2017). Perlindungan Privasi dan Data Pribadi Konsumen Daring Pada Online Marketplace System. *Justitia Jurnal Hukum*, *1*(2). https://doi.org/10.30651/justitia.v1i2.1152

Lobschat, L., Mueller, B., Eggers, F., Brandimarte, L., Diefenbach, S., Kroschke, M., & Wirtz, J. (2021). Corporate digital responsibility. *Journal of Business Research*, *122*(July 2018), 875–888. https://doi.org/10.1016/j.jbusres.2019.10.006

Moleong, L. J. (2017). Metode Penelitian Kualitatif. In *Edisi 36*. Bandung : PT. Remaja Rosdakarya Offset.

Muhammad, M. O., & Nugroho, L. D. (2021). Perlindungan Hukum Terhadap Pengguna Aplikasi E-Commerce yang Terdampak Kebocoran Data Pribadi. *Pamator Journal*, *14*(2), 165–174. https://doi.org/10.21107/pamator.v14i2.12472

Nugroho, A. A., Winanti, A., & Surahmad, S. (2020). Personal Data Protection in Indonesia: Legal Perspective. *International Journal of Multicultural and Multireligious Understanding*, *7*(7), 183. https://doi.org/10.18415/ijmmu.v7i7.1773

Putri, E. P., & Martha, A. E. (2021). The Importance of Enacting Indonesian Data Protection Law as a Legal Responsibility for Data Leakage. *Varia Justicia*, *17*(3), 287–303.

Rahmatullah, T. (2017). Analisis Permasalahan Hukum E-Commerce dan Pengaturannya di Indonesia. *Jurnal Hukum Media Justitia Nusantara*, *7*(2), 10–23. https://doi.org/10.13140/RG.2.2.27189.52967

Rahmi Ayunda, U. A. (2021). Perlindungan Data Diri Peminjam Dalam Transaksi Pinjaman Online: Kajian Perspektif Perlindungan Konsumen Di Indonesia. *E-Jurnal Komunitas Yustisia Universitas Pendidikan Ganesha*, *4*(3), 2.

Ratnasari, I., Siregar, S., & Maulana, A. (2021). How to build consumer trust towards e-satisfaction in e-commerce sites in the covid-19 pandemic time? *International Journal of Data and Network Science*, *5*(2), 127–134. https://doi.org/10.5267/j.ijdns.2021.2.001

Riyadi, G. A., & Toto Tohir Suriaatmadja. (2023). Perlindungan Hukum Atas Kebocoran Data Pribadi Konsumen PT PLN Dihubungkan Dengan Hak Atas Keamanan Pribadi Ditinjau Dari Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi. *Bandung Conference Series: Law Studies*, *3*(1). https://doi.org/10.29313/bcsls.v3i1.4945

Rohendi, A. (2015). Perlindungan Konsumen Dalam Transaksi E-Commerce Perspektif Hukum Nasional Dan Internasional. *Ecodemica*, *3*(2), 474–488.

Salim, S. C., & Neltje, J. (2022). Analysis of Legal Protection Towards Personal Data in E-Commerce. *Proceedings of the 3rd Tarumanagara International Conference on the Applications of Social Sciences and Humanities (TICASH 2021)*, *655*(Ticash 2021), 639–646. https://doi.org/10.2991/assehr.k.220404.101

Satrio, M. B., & Widiatno, M. W. (2020). Perlindungan Hukum Terhadap Data Pribadi Dalam Media Elektronik (Analisis Kasus Kebocoran Data Pengguna Facebook Di Indonesia). *JCA of Law*, *1*(1), 49–61.

Setiawati, D., Hakim, H. A., & Yoga, F. A. H. (2020). Optimizing Personal Data Protection in Indonesia: Lesson Learned from China, South Korea, and Singapore. *Indonesian Comparative Law Review*, *2*(2), 2–9. https://doi.org/10.18196/iclr.2219

Sinaga, E. N., Simanjuntak, B., Barus, L. B., & Sinaga, H. D. P. (2020). Reconstruction of E-Commerce Law in Addressing the Challenges of E-Commerce in Indonesia: A Fairness Perspective. *Ayer Journal*, *27*(2), 100–118.

Sonjaya, A., & Setiawan, D. A. (2022). Perlindungan Hukum bagi Korban Kebocoran Data Pribadi Pengguna Aplikasi Tokopedia berdasarkan UU No . 19 Tahun 2016 tentang Perubahan Atas UU No . 11 Tahun 2008 tentang Informasi dan Transaksi. *Law Studies*, *2*(19), 420–427.

Sulistiyono, A. (2022). *Legal Protection Against Leakage of Traveloka Consumer Personal Data by the Company*. 394–399.

Sylfia, A., Adyana, I. G. N., Amrullah, M. F., & Djaja, H. (2021). Tanggungjawab Yuridis PT. Tokopedia atas Kebocoran Data Pribadi dan Privasi Konsumen Dalam Transaksi Online. *Bhirawa Law Journal*, *2*(1), 21–27. https://doi.org/10.26905/blj.v2i1.5850

van Ooijen, I., & Vrabec, H. U. (2019). Does the GDPR Enhance Consumers' Control over Personal Data? An Analysis from a Behavioural Perspective. *Journal of Consumer Policy*, *42*(1), 91–107. https://doi.org/10.1007/s10603-018-9399-7