



PERLINDUNGAN HUKUM TERHADAP KORBAN PENYALAHGUNAAN DATA PRIBADI DALAM TRANSAKSI *E-COMMERCE* DENGAN METODE *CASH ON DELIVERY* (COD) BERDASARKAN UNDANG-UNDANG NOMOR 27 TAHUN 2022 TENTANG PERLINDUNGAN DATA PRIBADI (Studi Kasus: Kp. Pakem Selamat, Desa Petir, Kabupaten Serang)

Natasha Apriliani¹, Dika Ratu Marfu'atun², Fathullah³, Robby Nurtresna⁴
^{1,2,3,4}Universitas Primagraha, Indonesia

Email: acaaprilia091@gmail.com

Abstrak

Perkembangan teknologi informasi telah memicu meningkatnya transaksi perdagangan elektronik, termasuk sistem *cash on delivery* (COD). Di balik kemudahannya, praktik tersebut menyimpan potensi penyalahgunaan data pribadi konsumen, seperti nama, alamat, nomor telepon, dan rincian transaksi. Penelitian ini bertujuan mengidentifikasi ragam penyalahgunaan data pribadi pada transaksi *e-commerce* metode COD di Kampung Pakem Selamat, Desa Petir, Kabupaten Serang, serta mengkaji pertanggungjawaban hukum sebagai bentuk perlindungan bagi korban berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Metode yang digunakan adalah yuridis normatif dengan pendekatan empiris dan spesifikasi deskriptif analitis. Data dihimpun melalui studi kepustakaan serta wawancara dengan korban, kurir, dan pemilik toko daring, lalu dianalisis secara kualitatif. Temuan penelitian menunjukkan tiga modus penyalahgunaan data pribadi: penyamaran menjadi kurir dengan teknik social engineering, pemanfaatan identitas korban untuk pengiriman paket fiktif, serta phishing dengan mengaku sebagai petugas verifikasi untuk mendapatkan kode OTP. Perbuatan tersebut dapat memunculkan pertanggungjawaban pidana sebagaimana diatur dalam Pasal 65 dan Pasal 67 UU PDP, serta pertanggungjawaban administratif bagi Pengendali dan/atau Pemroses Data Pribadi yang tidak memenuhi kewajibannya. Simpulan penelitian, kerangka perlindungan hukum bagi korban telah tersedia secara normatif, namun implementasinya terkendala oleh kesulitan identifikasi pelaku, pembuktian asal kebocoran data, mekanisme kompensasi, dan rendahnya literasi digital masyarakat. Karena itu perlu penguatan sistem pengamanan data, pengawasan, sinergi aparat penegak hukum, dan peningkatan literasi digital.

Kata Kunci: *Perlindungan Hukum, Data Pribadi, E-Commerc, Cash On Delivery (COD), UU Perlindungan Data Pribadi*

Abstract

Advancements in information technology have spurred a rise in electronic commerce transactions, including the Cash On Delivery (COD) system. Despite its convenience, this practice carries the risk of personal data misuse involving details such as names, addresses, phone numbers, and transaction specifics. This study aims to identify the



various forms of personal data misuse in COD e-commerce transactions in Kampung Pakem Selamat, Petir Village, Serang Regency, and to examine legal liability as a form of victim protection under Law Number 27 of 2022 concerning Personal Data Protection (PDP Law). The study employs a normative-juridical method with an empirical approach and a descriptive-analytical specification. Data were gathered through literature reviews and interviews with victims, couriers, and online shop owners, followed by qualitative analysis. The findings reveal three modes of personal data misuse: impersonating a courier using social engineering techniques, using victims' identities to send fictitious packages, and phishing by posing as verification officers to obtain One-Time Password (OTP) codes. These actions can trigger criminal liability as stipulated in Articles 65 and 67 of the PDP Law, as well as administrative liability for Personal Data Controllers and/or Processors who fail to fulfill their obligations. The study concludes that while a normative legal protection framework for victims exists, its implementation is hindered by difficulties in identifying perpetrators, proving the source of data leaks, navigating compensation mechanisms, and low public digital literacy. Therefore, there is a need to strengthen data security systems and oversight, foster synergy among law enforcement agencies, and improve digital literacy.

Keywords: *Legal Protection, Personal Data, E-Commerce, Cash On Delivery (COD), Personal Data Protection Law.*

PENDAHULUAN

Kemajuan teknologi informasi dan komunikasi di era digital telah menimbulkan perubahan besar pada berbagai bidang kehidupan masyarakat. Kemajuan teknologi tersebut mendorong pemanfaatan sistem elektronik secara luas di berbagai sektor, salah satunya dalam kegiatan perdagangan elektronik atau *e-commerce*.¹ *E-commerce* memungkinkan transaksi berlangsung dengan tingkat efektivitas dan efisiensi yang lebih tinggi, tanpa terikat oleh batasan ruang maupun waktu. Sistem ini meliputi kegiatan pengumpulan, penyimpanan, pengolahan, hingga pendistribusian data dan informasi antara pelaku usaha dengan konsumen. Dengan demikian, kehadiran *e-commerce* tidak sekadar mengubah pola perdagangan konvensional, melainkan juga turut membentuk struktur mekanisme ekonomi digital yang lebih modern dan efisien.

Perdagangan digital di Indonesia mengalami pertumbuhan yang sangat cepat dalam sepuluh tahun terakhir seiring dengan meningkatnya penetrasi internet hingga 78% pada tahun 2023 dan semakin aktifnya konsumen di ranah daring.² Untuk mengatur perkembangan ini, pemerintah telah menetapkan beberapa peraturan utama, yaitu Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen, serta Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Secara teori, peraturan-peraturan tersebut bertujuan memberikan kepastian hukum bagi pelaku usaha dan konsumen. Namun dalam praktiknya masih banyak kendala

¹ Danvrianto Budhijanto, *Hukum Perlindungan Data Pribadi di Indonesia (Cyberlaw & Cybersecurity)*, PT Refika Aditama, Bandung, 2023, hlm. 111.

² Robby Nurtresna, "Legal Analysis of Digital Trade in Indonesia Based on Law Number 11 of 2008 concerning Electronic Information and Transactions", *Fox Justi: Jurnal Ilmu Hukum*, Vol. 15, No. 2, 2025, hlm. 290.



yang muncul, seperti multitafsir terhadap norma hukum, lemahnya pengawasan, dan belum memadainya infrastruktur pendukung. Buktinya, Badan Keamanan Siber dan Kriptografi Nasional mencatat lebih dari 2.000 insiden kebocoran data pribadi pada tahun 2022 di platform digital, termasuk yang melibatkan pelaku *e-commerce* besar, padahal Peraturan Pemerintah Nomor 71 Tahun 2019 mewajibkan penyedia platform untuk memastikan keamanan data pengguna. Hal ini menunjukkan adanya kesenjangan yang cukup besar antara regulasi yang ada dan implementasinya di lapangan.³

Secara yuridis, perlindungan konsumen di Indonesia diatur dalam Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen. Undang-undang tersebut mendefinisikan perlindungan konsumen sebagai upaya sistematis untuk mewujudkan adanya kepastian hukum guna melindungi hak-hak konsumen.⁴ Pasal 1 Angka 2 Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen memberikan pengertian bahwa: "Konsumen adalah setiap subjek hukum pemakai barang dan/atau jasa yang ada dalam masyarakat, diperuntukkan bagi kepentingan diri sendiri, keluarga, orang lain, atau makhluk hidup lain dan tidak untuk diperdagangkan."⁵ Bentuk perlindungan hukum bagi konsumen dalam Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen diantaranya berupa pengakuan hak dan kewajiban konsumen, serta jaminan kepastian hukum dalam memperoleh barang dan/atau jasa yang aman, akurat, dan sesuai dengan kesepakatan.⁶

Seiring berkembangnya teknologi digital, pengaturan mengenai perlindungan data pribadi kemudian diatur secara khusus melalui Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Berdasarkan Pasal 1 Angka 1 Undang-Undang Nomor 27 Tahun 2022, mendefinisikan pengertian data pribadi. Data pribadi diartikan sebagai seluruh informasi mengenai seseorang yang sudah dikenali dan berpotensi dapat dikenali, baik secara eksplisit maupun implisit melalui media elektronik maupun non-elektronik.⁷

Pada praktik transaksi *e-commerce*, metode pembayaran yang umum di implementasikan dalam aktivitas ekonomi masyarakat ialah metode *cash on delivery* (COD). Sistem pembayaran ini dilakukan pada saat barang diterima oleh pembeli. Dalam mekanisme ini, kurir atau jasa pengiriman bertindak sebagai perantara yang menyerahkan barang sekaligus menerima pembayaran dari pembeli untuk kemudian diteruskan kepada penjual.⁸ Di sisi lain, pada pembayaran ini, melibatkan pertukaran data pribadi antara pembeli dan penjual, seperti alamat dan nomor telepon. Kondisi tersebut membuka peluang terjadinya penyalahgunaan data pribadi, terutama apabila data tersebut digunakan tanpa persetujuan pemiliknya oleh pihak tertentu.

Permasalahan tersebut juga ditemukan di Kampung Pakem Selamat, Desa Petir, Kabupaten Serang. Berdasarkan hasil wawancara awal yang dilakukan penulis,

³ *Ibid*, hlm. 291.

⁴ Mod. Yusuf Daeng, Siti Yulia Makinninnawa, M. Fadly Daeng Yusuf, *Hukum Perlindungan Konsumen*, Taman Karya, Pekanbaru, 2024, hlm.17.

⁵ Robby Nurtresna, "Tinjauan Yuridis Perlindungan Hukum Bagi Konsumen Jasa Pengobatan Tradisional", *DESANTA Indonesian Of Interdisciplinary Journal*, Vol.2 No. 2, 2022, hlm. 220.

⁶ Dika Ratu Marfu'atun, "Perlindungan Konsumen terhadap Penggunaan Klausula Baku tentang Pemberian Kuasa dalam Perjanjian Kredit Bank di PT Bank Pembangunan Daerah Jawa Barat dan Banten Tbk Kantor Cabang Khusus Banten", *Nurani Hukum: Jurnal Ilmu Hukum*, Vol. 3, No.1. 2020, hlm. 65.

⁷ Sinta Dwi Rosadi, *Pembahasan UU Perlindungan Data Pribadi (UU RI No.27 Tahun 2022)*, Sinar Grafika, Jakarta, 2023, hlm.27.

⁸ Richardus Eko Indrajit, *E-Commerce: Strategi dan Konsep Bisnis Digital*, Andi, Yogyakarta, 2021, hlm. 85.



ditemukan beberapa kasus penyalahgunaan data pribadi dalam transaksi *e-commerce* dengan metode COD melalui platform TikTok Shop. Salah satunya dialami oleh Saudari Lia yang menjadi korban penipuan oleh seseorang yang mengaku sebagai kurir J&T dan mengetahui rincian pesannya. Korban kemudian membayar sebesar Rp200.000 kepada kurir palsu tersebut sebelum mengetahui bahwa kurir yang datang bukanlah kurir sebenarnya. Kasus lainnya dialami oleh Saudari Manda, yang keluarganya menerima dan membayar paket COD atas namanya sebesar Rp250.000, meskipun Manda tidak pernah melakukan pemesanan. Sementara itu, Ibu Neneng mengalami penyalahgunaan data yang lebih lanjut ketika pelaku mengetahui rincian pesanan COD miliknya dan menghubungkannya dengan mengaku sebagai petugas verifikasi. Pelaku kemudian memperoleh kode akses sekali pakai dari korban dan menggunakannya untuk melakukan transaksi sebesar Rp300.000 tanpa persetujuan korban.

Ketiga kasus tersebut menunjukkan adanya bentuk penyalahgunaan data pribadi yang berbeda, mulai dari penggunaan nama dan alamat untuk pesanan yang tidak dilakukan korban, penyamaran sebagai kurir dengan memanfaatkan informasi pesanan, hingga penggunaan informasi transaksi untuk melakukan penipuan dan memperoleh akses terhadap dana korban. Kondisi tersebut menunjukkan adanya kesenjangan antara perlindungan hukum yang secara normatif telah diberikan melalui Undang-Undang Nomor 27 Tahun 2022 dengan kondisi faktual yang masih memungkinkan terjadinya penyalahgunaan data pribadi dalam transaksi *e-commerce*.

Permasalahan tersebut penting untuk dikaji karena perlindungan data pribadi tidak hanya berkaitan dengan keamanan informasi, tetapi juga menyangkut perlindungan hak dan kepentingan korban ketika data pribadinya disalahgunakan. Oleh karena itu, penelitian ini mengkaji bentuk penyalahgunaan data pribadi dalam transaksi *e-commerce* dengan metode COD yang terjadi di Kampung Pakem Selamat, Desa Petir, Kabupaten Serang, serta menganalisis tanggung jawab hukum terhadap penyalahgunaan tersebut sebagai bentuk perlindungan hukum bagi korban berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.

METODE PENELITIAN

Penelitian ini menggunakan metode yuridis normatif dengan didukung pendekatan empiris. Spesifikasi penelitian bersifat deskriptif analitis untuk menggambarkan dan menganalisis penyalahgunaan data pribadi dalam transaksi *e-commerce* dengan metode *cash on delivery* (COD). Data yang digunakan terdiri atas data primer dan data sekunder. Data primer diperoleh melalui wawancara dengan korban, kurir, dan pemilik toko online di TikTok Shop.

Data sekunder diperoleh melalui studi kepustakaan berupa peraturan perundang-undangan, buku, dan jurnal ilmiah. Bahan hukum primer meliputi Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen, dan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik beserta perubahannya.

Teknik pengumpulan data dilakukan melalui studi kepustakaan dan wawancara. Data dianalisis secara kualitatif dengan menghubungkan fakta di lapangan dengan ketentuan hukum dan teori yang relevan. Analisis dilakukan untuk menjawab permasalahan mengenai penyalahgunaan dan pertanggungjawaban hukum terhadap data



pribadi. Penelitian dilaksanakan di Kampung Pakem, Desa Petir, Kabupaten Serang, Provinsi Banten.

HASIL DAN PEMBAHASAN

A. Bentuk-Bentuk Penyalahgunaan Data Pribadi dalam Transaksi *E-commerce* dengan Metode *Cash On Delivery* (COD) di Kampung Pakem Selamat, Desa Petir, Kabupaten Serang

Perkembangan *e-commerce* memberikan kemudahan dalam memperoleh barang dan jasa karena transaksi dapat dilakukan secara cepat, fleksibel, dan tanpa batasan ruang maupun waktu. Namun, kemudahan tersebut juga menimbulkan risiko penyalahgunaan data pribadi. Data berupa nama, alamat, nomor telepon, dan informasi transaksi dapat dimanfaatkan oleh pihak yang tidak berwenang untuk melakukan penipuan, pencurian identitas, maupun pelanggaran privasi.

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi memberikan dasar hukum terhadap perlindungan data pribadi dan melarang penggunaan data secara melawan hukum. Salah satunya diatur dalam Pasal 66 yang melarang setiap orang membuat atau memalsukan data pribadi untuk memperoleh keuntungan yang dapat menimbulkan kerugian bagi orang lain. Dalam transaksi *e-commerce*, penyalahgunaan data dapat berupa penggunaan data tanpa persetujuan, kebocoran data, pencurian identitas, paket COD fiktif, penyamaran sebagai kurir atau layanan pelanggan, phishing, penjualan data kepada pihak ketiga, pemalsuan data, serta penyalahgunaan oleh pihak internal.

Berdasarkan hasil penelitian di Kampung Pakem Selamat, Desa Petir, Kabupaten Serang, ditemukan tiga bentuk penyalahgunaan data pribadi dalam transaksi *e-commerce* dengan metode *cash on delivery* (COD), yaitu penyamaran sebagai kurir, paket COD fiktif, dan *phishing*.

1. Kasus Saudari Lia

Saudari Lia mengalami penyalahgunaan data pribadi dalam bentuk penyamaran sebagai kurir atau *social engineering*. Berdasarkan hasil wawancara, sebelum kurir resmi J&T datang, seseorang mengaku sebagai kurir dan membawa paket atas nama Lia. Pelaku mengetahui nama, alamat, serta barang yang dipesan melalui TikTok Shop sehingga korban percaya bahwa pelaku merupakan kurir yang sah. Korban kemudian membayar sebesar Rp200.000,00. Tidak lama kemudian, kurir resmi datang membawa paket yang sebenarnya, sehingga korban menyadari telah menjadi korban penipuan.

Kasus tersebut menunjukkan bahwa data pribadi berupa identitas, alamat, dan informasi pesanan digunakan pelaku untuk membangun kepercayaan korban dan melakukan penyamaran. Dengan demikian, data pribadi tidak hanya berfungsi sebagai identitas, tetapi juga dapat digunakan sebagai sarana manipulasi untuk memperoleh keuntungan secara melawan hukum.

2. Kasus Saudari Manda

Saudari Manda mengalami penyalahgunaan data pribadi dalam bentuk paket COD fiktif. Berdasarkan hasil wawancara, ketika korban sedang bekerja, orang tuanya menerima paket COD atas nama Manda dan membayar Rp250.000,00 karena mengira barang tersebut merupakan pesanan korban. Setelah mengetahui kejadian tersebut, Manda memeriksa akun *e-commerce* dan menemukan bahwa



tidak terdapat pesanan yang dibuat olehnya. Setelah menghubungi toko, diketahui terdapat pesanan atas namanya dan alamat yang sama, tetapi menggunakan nomor telepon yang berbeda.

Peristiwa tersebut menunjukkan bahwa nama dan alamat korban digunakan tanpa persetujuan untuk membuat transaksi fiktif. Penggunaan metode *cash on delivery* (COD) menyebabkan paket tetap dikirim ke alamat korban dan pembayaran dilakukan oleh anggota keluarga. Kasus ini memperlihatkan bahwa penyalahgunaan data pribadi dapat menimbulkan kerugian materiil meskipun akun e-commerce korban tidak diambil alih.

3. Kasus Ibu Neneng

Ibu Neneng mengalami penyalahgunaan data pribadi dalam bentuk *phishing* yang dilakukan melalui penyamaran sebagai petugas verifikasi pesanan. Berdasarkan hasil wawancara, pelaku mengetahui nama, alamat, nomor telepon, dan barang yang dipesan korban melalui TikTok Shop. Pelaku kemudian menghubungi korban dan meminta kode *One-Time Password* (OTP) dengan alasan untuk memperbaiki masalah pada pesanan. Setelah kode diberikan, saldo rekening korban berkurang sebesar Rp300.000,00.

Kasus tersebut menunjukkan bahwa data pribadi korban digunakan untuk memperoleh kepercayaan sebelum pelaku meminta informasi autentikasi berupa kode OTP. Data pribadi yang telah dikuasai pelaku menjadi sarana untuk melakukan *social engineering*, sedangkan kode OTP digunakan untuk melakukan transaksi tanpa izin. Dengan demikian, penyalahgunaan data pribadi dalam kasus ini tidak hanya menimbulkan pelanggaran terhadap privasi, tetapi juga kerugian finansial bagi korban.

Berdasarkan ketiga kasus tersebut, dapat diketahui bahwa penyalahgunaan data pribadi dalam metode *cash on delivery* (COD) di Kampung Pakem Selamat memiliki pola yang berbeda, yaitu penggunaan data untuk menyamar sebagai kurir, membuat pesanan COD fiktif, dan melakukan *phishing* untuk memperoleh kode OTP. Ketiganya menunjukkan bahwa data pribadi berupa nama, alamat, nomor telepon, dan informasi transaksi dapat menjadi sarana bagi pelaku untuk memperoleh kepercayaan korban dan melakukan tindakan yang merugikan. Kondisi tersebut menunjukkan pentingnya perlindungan dan keamanan data pribadi dalam setiap tahapan transaksi *e-commerce*.

B. Pertanggungjawaban Hukum atas Penyalahgunaan Data Pribadi dalam Transaksi *E-commerce* dengan Metode *Cash On Delivery* (COD) sebagai Bentuk Perlindungan Hukum Bagi Korban berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

1. Langkah Awal yang dapat di tempuh korban

Korban penyalahgunaan data pribadi dalam transaksi COD sebaiknya segera melakukan langkah-langkah awal untuk meminimalkan kerugian serta mempermudah proses pembuktian apabila perkara dilanjutkan melalui jalur hukum. Sebelum mendapatkan pertanggungjawaban hukum, korban penyalahgunaan data pribadi dalam transaksi *e-commerce* dengan metode COD, Langkah-langkah yang dapat dilakukan korban meliputi :

- a) Mengumpulkan seluruh bukti yang berkaitan dengan peristiwa penyalahgunaan data pribadi



Bukti-bukti tersebut seperti tangkapan layar percakapan, rekaman panggilan telepon, nomor telepon pelaku, bukti transaksi pada platform *e-commerce*, resi pengiriman, hingga identitas akun yang digunakan pelaku. Bukti-bukti tersebut memiliki nilai penting karena sebagian besar tindak penyalahgunaan data pribadi dilakukan melalui media elektronik sehingga pembuktiannya sangat bergantung pada bukti digital.

b) Menghubungi pemilik toko dimana barang itu di pesan;

Apabila ada indikasi penyalahgunaan data oleh toko online langkah yang dapat di tempuh yaitu mengajukan pengaduan kepada pemilik toko online. Sebagaimana hasil Berdasarkan wawancara penulis dengan pemilik salah satu toko online di platform TiktokShop, diketahui bahwa jika ada konsumen yang melaporkan penyalahgunaan data pribadi, toko akan melakukan pengecekan terhadap riwayat transaksi dan pihak yang memiliki akses terhadap data tersebut. Dari keterangan narasumber pengaduan langsung kepada toko dapat menjadi langkah awal bagi korban.

c) Mengajukan pengaduan kepada perusahaan ekspedisi;

Apabila ada indikasi penyalahgunaan data oleh kurir atau petugas pengiriman langkah yang dapat di tempuh yaitu mengajukan pengaduan kepada perusahaan ekspedisi. Sebagaimana hasil wawancara peneliti dengan salah satu kurir ekspedisi JNT menunjukkan bahwa tugas kurir sebatas mengantarkan barang sesuai data yang disediakan sistem perusahaan. Apabila ada laporan terkait penyalahgunaan data pribadi, perusahaan ekspedisi akan melakukan pemeriksaan terhadap petugas yang menangani pengiriman. Menurut narasumber, perusahaan jasa pengiriman juga menyediakan mekanisme pengaduan bagi pelanggan sebagai upaya penyelesaian sebelum perkara dibawa ke ranah hukum.

d) Menempuh musyawarah untuk mencapai kesepakatan dan ganti rugi secara sukarela.

e) Melaporkan kepada aparat penegak hukum apabila mediasi tidak mencapai kesepakatan atau terdapat unsur pidana.

Korban dapat membuat laporan kepada Kepolisian Republik Indonesia apabila terdapat dugaan tindak pidana penyalahgunaan data pribadi, penipuan, atau akses ilegal terhadap data. Laporan tersebut menjadi dasar dilakukannya penyelidikan dan penyidikan

Langkah-langkah yang telah diuraikan di atas merupakan upaya awal yang dapat ditempuh korban untuk melindungi hak-haknya setelah terjadi penyalahgunaan data pribadi dalam transaksi *e-commerce* dengan metode *cash on delivery* (COD). Namun, apabila penyalahgunaan data pribadi tersebut terbukti menimbulkan kerugian atau dilakukan dengan melanggar ketentuan peraturan perundang-undangan, maka pihak yang bertanggung jawab dapat dimintai pertanggungjawaban hukum. Pertanggungjawaban tersebut dapat berupa sanksi administratif terhadap pihak yang lalai memenuhi kewajiban perlindungan data pribadi, tanggung jawab perdata berupa kewajiban memberikan ganti kerugian kepada korban, maupun pertanggungjawaban pidana apabila perbuatan tersebut memenuhi unsur tindak pidana sebagaimana diatur dalam Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Oleh karena itu, pembahasan



selanjutnya akan menguraikan bentuk-bentuk pertanggungjawaban hukum administratif, dan pertanggungjawaban hukum pidana sebagai wujud perlindungan hukum bagi korban.

2. Pertanggungjawaban Hukum Terhadap Korban Penyalahgunaan Data Pribadi dalam Transaksi *E-commerce* dengan Metode *Cash On Delivery* (COD) berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

Tanggung jawab hukum dalam konteks pengelolaan data pribadi merujuk pada kewajiban pelaku usaha atau pihak terkait untuk memastikan keamanan data dan memenuhi hak-hak konsumen. Prinsip *legal compliance* menuntut perusahaan untuk mengelola data sesuai dengan ketentuan hukum yang berlaku.⁹

Undang-Undang Perlindungan Data Pribadi menetapkan bahwa pengendali data wajib menerapkan langkah-langkah preventif guna menjaga kerahasiaan data, menyampaikan pemberitahuan apabila terjadi insiden pelanggaran, serta menyediakan mekanisme pemulihan. Kewajiban tersebut dapat menimbulkan konsekuensi administratif, maupun pidana, tergantung pada tingkat dan sifat pelanggaran yang terjadi.¹⁰

a. Pertanggungjawaban Administratif

Pada praktik transaksi elektronik, data pribadi milik konsumen dikelola oleh banyak pihak. Mulai dari pengelola platform marketplace, pelaku usaha yang berjualan, jasa pengiriman, hingga pihak-pihak lain yang diberi akses terhadap data itu. Merujuk pada Undang-undang Perlindungan Data Pribadi, baik pengendali data maupun pemroses data dibebani tanggung jawab untuk memastikan keamanan dan kerahasiaan data pribadi, sekaligus mencegah potensi penyalahgunaannya.

Pasal 35 menegaskan bahwa:

“Pengendali Data Pribadi wajib melindungi dan memastikan keamanan Data Pribadi yang diprosesnya.”¹¹

Pasal 36 mengatur bahwa:

“Pengendali Data Pribadi wajib melakukan pengawasan terhadap setiap pihak yang terlibat dalam pemrosesan Data Pribadi di bawah kendalinya.”

Berdasarkan ketentuan tersebut, jika kebocoran data pribadi konsumen terjadi akibat lemahnya sistem pengamanan atau adanya kelalaian dari pengendali data, maka pengendali data dapat dikenai pertanggungjawaban administratif. Pertanggungjawaban administratif dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi dibebankan kepada Pengendali Data Pribadi dan/atau Pemroses Data Pribadi yang tidak memenuhi kewajiban perlindungan data. Dalam transaksi *e-commerce* dengan metode COD, tanggung jawab tersebut tidak dibebankan kepada pelaku penyalahgunaan,

⁹ Hendra Saputra, dkk. “Analisis Tanggung Jawab Etis dan Hukum Perusahaan E-Commerce terhadap Perlindungan Data Pribadi Konsumen: Studi Kasus Kebocoran Data Tokopedia 2020”, SCIENTIFIC JOURNAL OF REFLECTIO : Economic, Accounting, Management and Business, Vol. 9, No. 1, January 2026, hlm. 122.

¹⁰ *Ibid*, hlm. 123.

¹¹ Sinta Dewi Rosadi, *Op-Cit*, hlm. 125



melainkan kepada pihak yang secara hukum wajib mengelola dan mengamankan data konsumen.

Kebocoran atau penyalahgunaan data dapat timbul akibat sistem keamanan yang lemah, minimnya pengawasan, atau tidak diterapkannya standar perlindungan. Pada praktik COD, data berupa nama, alamat, dan nomor telepon diproses oleh marketplace, pelaku usaha, dan jasa pengiriman. Oleh karena itu, setiap Pengendali Data wajib memastikan data hanya digunakan sesuai tujuan dan terlindungi dari akses pihak tidak berwenang.

Pengendali Data Pribadi dapat dikenai sanksi administratif apabila terbukti adanya kelalaian, seperti tidak menyediakan sistem keamanan yang memadai, tidak melakukan pengawasan terhadap pihak pemroses data di bawah kendalinya, atau membiarkan data pribadi dapat diakses pihak tidak berwenang sehingga disalahgunakan dalam modus penipuan COD. Ketentuan ini sebagaimana diatur dalam Pasal 57 ayat (1) UU PDP Menyebutkan bahwa:

“Pelanggaran terhadap ketentuan tertentu dalam Undang-Undang ini dapat dikenai sanksi administratif.”

Ketentuan mengenai sanksi administratif akibat pelanggaran data pribadi ditegaskan dalam UU Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi beserta aturan turunannya. Jenis sanksinya mencakup:

- 1) Pemberian peringatan, baik secara lisan maupun tertulis, kepada pihak pengelola data pribadi yang melakukan pelanggaran.
- 2) Penundaan sementara kegiatan pengolahan data pribadi yang tidak mematuhi peraturan.
- 3) Penghapusan atau pemusnahan data pribadi hasil pemrosesan yang melanggar hukum.
- 4) Denda administratif hingga 2% dari pendapatan tahunan pengelola data pribadi berdasarkan variabel pelanggaran.¹²

Penerapan sanksi administratif bertujuan untuk menimbulkan efek deterren sekaligus mendorong Pengendali Data Pribadi agar menjalankan kewajiban pengelolaan data dengan prinsip kehati-hatian dan akuntabilitas.¹³ Secara konseptual, sanksi administratif memiliki dua fungsi utama, yakni fungsi preventif dan fungsi represif. Fungsi preventif berperan dalam mendorong kepatuhan Pengendali Data terhadap ketentuan perlindungan data pribadi sejak tahap awal pemrosesan. Sementara itu, fungsi represif dimaksudkan untuk memberikan efek jera sehingga praktik pelanggaran serupa tidak terulang. Dengan demikian, diharapkan sistem pengelolaan data pribadi menjadi lebih terjamin keamanannya dan kredibel, sehingga dapat meningkatkan rasa aman masyarakat dalam setiap aktivitas di ruang digital.

¹² Shafa Salsabila dan Sido Ahyar Wiraguna, “Pertanggungjawaban. Hukum atas Pelanggaran Data Pribadi dalam Perspektif Undang-Undang Pelindungan Data Pribadi Indonesia”. *Konsensus: Jurnal Ilmu Pertahanan, Hukum dan Ilmu Komunikasi*, Vol. 2, No. 2, 2025. hlm.152.

¹³ Ajeng Nur Annisa, *Konsumen Digital dan Perlindungan Hukum di Indonesia*, CV. Adanu Abimata, Indramayu, 2026, hlm.63.



Dalam ekosistem transaksi *e-commerce* berbasis COD, pihak-pihak yang dapat dijatuhi sanksi administratif oleh pemerintah jika terbukti lalai atau sengaja menyalahgunakan data meliputi:

- 1) Penyelenggara Perdagangan Melalui Sistem Elektronik (Platform *E-Commerce*): Bertindak sebagai Pengendali Data Pribadi. Mereka dapat disanksi jika terbukti memiliki celah keamanan (*security breach*) yang menyebabkan data pengguna bocor, atau membiarkan penjual nakal memanfaatkan data pembeli tanpa verifikasi ketat.
- 2) Pelaku Usaha atau Penjual (*Merchant*): Baik perorangan maupun badan usaha yang membuka toko di *e-commerce*. Mereka disanksi jika terbukti memproses, menyimpan, atau menggunakan data alamat atau kontak korban untuk mengirimkan barang COD fiktif (tanpa persetujuan korban).
- 3) Perusahaan Jasa Ekspedisi atau Kurir: Jika mereka bertindak sebagai Prosesor Data atau Pengendali Data bersama yang terbukti membocorkan basis data alamat pelanggan kepada pihak ketiga demi keuntungan sepihak (misal untuk sindikat scam COD)

b. Pertanggungjawaban Pidana

Pertanggungjawaban Pidana dapat dikenakan terhadap setiap orang, badan hukum maupun organisasi internasional yang melakukan tindakan melawan hukum berupa mengumpulkan data digunakan untuk keuntungan diri sendiri maupun orang lain, mengungkap data yang bukan miliknya dan memalsukan data yang menyebabkan terjadinya kerugian terhadap orang lain.¹⁴ Pasal 67 ayat (1), ayat (2), dan ayat (3) UU Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi mengatur secara tegas pidana terkait penyalahgunaan data pribadi. Ketentuan tersebut menjadi tonggak penting dalam hukum pidana Indonesia untuk memperkuat perlindungan hak privasi sebagai hak asasi manusia. Atas pelanggaran tersebut, UU PDP menjatuhkan ancaman pidana sebagai berikut:

Pasal 67 ayat (1) :

“Setiap Orang yang dengan sengaja dan melawan hukum memperoleh atau mengumpulkan Data Pribadi yang bukan miliknya sebagaimana dimaksud dalam Pasal 65 ayat (1) dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau pidana denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah).”

Unsur delik ini mencakup: subjek “setiap orang” termasuk individu dan korporasi; adanya kesengajaan; sifat melawan hukum; perbuatan memperoleh atau mengumpulkan; objek berupa data pribadi orang lain; tujuan untuk keuntungan; dan potensi merugikan pemilik data.

Memperoleh data pribadi baru bisa dipidana kalau seluruh unsur tersebut terpenuhi, terutama unsur melawan hukum dan tujuan tertentu. Meski begitu, ada pengecualian untuk aktivitas pribadi atau lingkup rumah tangga yang tidak masuk ranah pidana.

Pasal 67 ayat (2) :

¹⁴ Tomi Wicaksono Putra, Hamidah Abdurrachman, dan Achmad Irwan Hamzani, *Pertanggungjawaban Pidana Terhadap Kejahatan Hacking*, PT Nasya Expanding Management, Pekalongan, 2023, hlm.7.



“Setiap Orang yang dengan sengaja dan melawan hukum mengungkapkan Data Pribadi yang bukan miliknya sebagaimana dimaksud dalam Pasal 65 ayat (2) dipidana dengan pidana penjara paling lama 4 (empat) tahun dan/atau pidana denda paling banyak Rp4.000.000.000,00 (empat miliar rupiah).”

Pada substansinya, unsur-unsur dalam ketentuan ini sama dengan yang diatur pada ayat (1). Letak perbedaannya ada pada jenis tindakannya, yaitu “mengungkapkan”, yang dapat dimaknai sebagai perbuatan memperlihatkan, membuka, atau menyebarluaskan data pribadi kepada pihak lain. Namun dalam penerapannya, ada beberapa pengecualian. Misalnya, apabila pemilik data sudah memberikan persetujuan atau pengungkapan tersebut dilakukan untuk tujuan tertentu yang dibenarkan peraturan perundang-undangan, khususnya bila menyangkut data yang tergolong sensitif.

Pasal 67 ayat (3) :

“Setiap Orang yang dengan sengaja dan melawan hukum menggunakan Data Pribadi yang bukan miliknya sebagaimana dimaksud dalam Pasal 65 ayat (3) dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau pidana denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah).”

Perbuatan “menggunakan” dalam konteks ini memiliki makna yang luas, mencakup segala bentuk pemanfaatan data untuk tujuan ekonomi, tindakan penipuan, atau kegiatan lain yang melanggar hukum. Kasus konkretnya dapat dilihat pada penyalahgunaan data dalam transaksi keuangan ilegal, misalnya pembobolan kartu kredit. Ketentuan tersebut menegaskan bahwa pemakaian data pribadi tanpa hak merupakan pelanggaran berat yang bisa dijatuhi sanksi pidana.

Secara umum, tiga aturan yang termuat dalam Pasal 67 itu adalah bentuk pemberian sanksi pidana terhadap seluruh rangkaian penyalahgunaan data pribadi, sejak tahap memperoleh, menyebarluaskan, hingga memanfaatkan data. Aturan ini merupakan jawaban hukum atas pesatnya perkembangan teknologi informasi serta meningkatnya ancaman terhadap privasi.¹⁵

Ancaman pidana pada ayat (1), ayat (2), dan ayat (3) Pasal 67 Undang-Undang Nomor 27 Tahun 2022 merumuskan frasa “dan/atau” di antara pidana penjara dan pidana denda. Penggunaan frasa tersebut menimbulkan konsekuensi yuridis berupa adanya tiga opsi pemidanaan yang dapat dijatuhkan oleh hakim, yaitu:

- 1) Dijatuhi pidana penjara saja tanpa pidana denda; atau,
- 2) Dijatuhi pidana denda saja tanpa pidana penjara; atau,
- 3) Dijatuhi pidana penjara dan pidana denda sekaligus.

¹⁵ Febrika Patricia Carolin Mamadoa, Herlyanty Y. A. & Bawole Yumi Simbala, “Larangan Dan Sanksi Atas Perolehan Dan Penggunaan Data Pribadi Secara Melawan Hukum Berdasarkan UU No 27 Tahun 2022 Tentang Perlindungan Data Pribadi”, Jurnal Fakultas Hukum Unsrat, Vol. 15, No. 3, 2026, hlm.3.



Penggunaan frasa “dan/atau” pada dua jenis pidana pokok, yaitu pidana penjara dan pidana denda, merupakan ketentuan khusus atau *Lex specialis* yang mengesampingkan ketentuan umum dalam KUHP atau hukum pidana umum. Salah satu prinsip dalam KUHP sebagai *lex generalis* menyatakan bahwa dua pidana pokok tidak boleh dijatuhkan secara kumulatif.¹⁶

3. Tantangan Implementasi Perlindungan Hukum Terhadap Penyalahgunaan Data Pribadi Dalam Transaksi *E-commerce* dengan Metode *Cash On Delivery* (COD)

Indonesia telah memiliki Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi sebagai dasar hukum perlindungan hak subjek data, implementasinya dalam praktik masih menghadapi berbagai tantangan. Dalam kasus penyalahgunaan data pribadi pada transaksi *e-commerce*, perlindungan hukum tidak hanya bergantung pada keberadaan norma hukum, tetapi juga pada efektivitas penegakan hukum, kemampuan mengidentifikasi pelaku, serta mekanisme pemulihan hak korban. Tantangan-tantangannya sebagai berikut:

a. Kesulitan dalam mengidentifikasi pelaku penyalahgunaan data pribadi.

Dalam praktiknya, pelaku umumnya menggunakan identitas palsu, nomor telepon yang tidak terdaftar atas nama sebenarnya, akun media sosial sementara, maupun rekening milik pihak lain sebagai sarana melakukan tindak pidana. Modus tersebut menyebabkan aparat penegak hukum mengalami kesulitan dalam melacak identitas pelaku maupun membuktikan pihak yang pertama kali memperoleh dan menyebarkan data pribadi korban. Akibatnya, meskipun korban mengetahui bahwa data pribadinya telah disalahgunakan, proses penyelidikan dan pembuktian sering kali memerlukan waktu yang lama serta bergantung pada kerja sama berbagai pihak, seperti penyelenggara sistem elektronik, dan perusahaan jasa pengiriman. Hambatan penegakan hukum serta lemahnya koordinasi antarlembaga masih menjadi salah satu tantangan utama implementasi Undang-Undang Perlindungan Data Pribadi.

b. Kesulitan pembuktian sumber kebocoran data pribadi.

Dalam transaksi *e-commerce* dengan metode *cash on delivery* (COD), data pribadi konsumen diproses oleh beberapa pihak, mulai dari penyelenggara platform, pelaku usaha, perusahaan jasa pengiriman, hingga pihak lain yang mendukung proses transaksi. Banyaknya pihak yang memiliki akses terhadap data menyebabkan sulit ditentukan dari mana data tersebut pertama kali bocor. Dalam banyak kasus, korban hanya mengetahui bahwa pelaku menguasai nama, alamat, nomor telepon, maupun rincian pesannya, tetapi tidak dapat membuktikan pihak yang lalai dalam menjaga keamanan data pribadi tersebut. Kondisi ini menyebabkan proses penegakan hukum menjadi lebih kompleks karena pembuktian mengenai hubungan antara kebocoran data dan kerugian yang dialami korban tidak mudah dilakukan.

c. Belum optimalnya mekanisme pemberian ganti rugi kepada korban.

Meskipun Undang-Undang Perlindungan Data Pribadi memberikan hak kepada subjek data untuk memperoleh perlindungan dan mengajukan tuntutan

¹⁶ A.P.A. Santoso et al, *Kapita Selekta Hukum Pidana Suatu Pengenalan Dasar*, Pustakabaru Press, Yogyakarta, 2022, hlm. 29.



atas kerugian yang dialaminya, dalam praktik korban masih mengalami kesulitan memperoleh kompensasi. Hal tersebut disebabkan karena pelaku sering kali tidak diketahui identitasnya, sehingga tidak terdapat pihak yang dapat dimintai pertanggungjawaban secara langsung. Di sisi lain, penyelenggara platform *e-commerce*, penjual maupun perusahaan jasa pengiriman pada umumnya hanya memberikan bantuan berupa penanganan pengaduan atau investigasi internal, tetapi tidak selalu memberikan ganti rugi atas kerugian materiil yang dialami korban. Akibatnya, korban sering kali harus menanggung sendiri kerugian yang timbul akibat penyalahgunaan data pribadinya. Kajian terbaru mengenai konsep ganti rugi dalam Undang-Undang Perlindungan Data Pribadi juga menunjukkan bahwa mekanisme kompensasi bagi korban masih menghadapi berbagai kendala dalam implementasinya sehingga belum memberikan kepastian hukum secara efektif.

- d. Rendahnya kesadaran masyarakat mengenai pentingnya perlindungan data pribadi juga menjadi faktor yang memengaruhi efektivitas perlindungan hukum

Sebagian masyarakat masih mudah memberikan informasi pribadi maupun kode verifikasi (*One Time Password/OTP*) kepada pihak yang mengaku sebagai petugas resmi tanpa melakukan verifikasi terlebih dahulu. Kondisi tersebut dimanfaatkan oleh pelaku melalui teknik *social engineering* untuk memperoleh keuntungan secara melawan hukum. Oleh karena itu, selain memperkuat penegakan hukum, diperlukan peningkatan literasi digital agar masyarakat mampu mengenali berbagai bentuk penyalahgunaan data pribadi dan tidak mudah menjadi korban kejahatan berbasis rekayasa sosial.

Berdasarkan uraian tersebut, dapat disimpulkan bahwa tantangan implementasi perlindungan hukum terhadap penyalahgunaan data pribadi dalam transaksi *e-commerce* tidak hanya terletak pada aspek pengaturan hukum, tetapi juga pada aspek penegakan hukum dan pemulihan hak korban. Sulitnya mengidentifikasi pelaku, rumitnya pembuktian asal kebocoran data, serta belum optimalnya mekanisme ganti rugi menyebabkan perlindungan hukum yang diberikan kepada korban belum sepenuhnya efektif. Oleh karena itu, diperlukan penguatan koordinasi antarlembaga, peningkatan sistem keamanan data oleh penyelenggara sistem elektronik, serta mekanisme penyelesaian sengketa yang mampu memberikan kepastian hukum dan pemulihan yang lebih efektif bagi korban penyalahgunaan data pribadi.

PENUTUP

A. Kesimpulan

Berdasarkan pemaparan penelitian ini, transaksi *e-commerce* dengan metode COD memang memberikan kemudahan, tetapi juga menimbulkan kerentanan terhadap penyalahgunaan data pribadi. Di Kampung Pakem Selamat, Desa Petir, Kabupaten Serang, tiga bentuk yang nyata terjadi adalah penyamaran sebagai kurir yang dialami Saudari Lia, penipuan COD melalui paket fiktif yang dialami Saudari Manda, dan *phishing* yang dialami Ibu Neneng. Untuk korban, langkah yang disarankan adalah segera mengumpulkan bukti, mengadukan masalah ke toko dan



perusahaan ekspedisi, menempuh musyawarah, serta melapor ke aparat penegak hukum apabila tidak ada penyelesaian. Pertanggungjawaban hukum atas kasus ini diatur dalam Undang-undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi. Undang-undang tersebut mencakup sanksi administratif bagi pengendali data yang lalai, ganti kerugian secara perdata, dan sanksi pidana berdasarkan Pasal 67 bagi pihak yang sengaja dan melawan hukum memperoleh, mengungkapkan, atau menggunakan data pribadi orang lain. Perlu diketahui UU PDP tidak menetapkan batas minimal kerugian, sehingga perkara tetap dapat diproses meskipun kerugian kecil.

Namun dalam praktiknya perlindungan hukum masih menghadapi kendala seperti sulitnya mengidentifikasi pelaku, rumitnya pembuktian asal kebocoran data, belum optimalnya mekanisme ganti rugi, serta rendahnya kesadaran masyarakat dalam menjaga data pribadi. Dengan demikian, efektivitas perlindungan hukum tidak hanya bergantung pada norma dalam Undang-undang, tetapi juga pada penegakan hukum, penguatan sistem keamanan, dan peningkatan literasi digital masyarakat.

B. Saran

Penulis merekomendasikan penguatan sistem dan penegakan hukum untuk menekan penyalahgunaan data pada transaksi COD. Platform *e-commerce*, pelaku usaha, dan jasa pengiriman perlu memperketat keamanan data dengan membatasi akses, meningkatkan pengawasan, dan menerapkan standar perlindungan agar tidak terjadi kebocoran. Masyarakat juga harus diedukasi agar lebih waspada menjaga data pribadi dan mengenali modus penipuan.

Dari sisi hukum, pemerintah dan aparat harus mengoptimalkan Undang-undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi melalui pengawasan ketat, peningkatan kemampuan forensik digital, dan koordinasi antar lembaga untuk melacak sumber kebocoran. Mekanisme penyelesaian sengketa dan ganti rugi bagi korban juga perlu disederhanakan agar pemulihan hak lebih mudah diakses. Tujuannya agar perlindungan hukum tidak hanya memberi sanksi, tetapi benar-benar memulihkan kerugian korban.

DAFTAR PUSTAKA

BUKU :

- Ajeng Nur Annisa, *Konsumen Digital dan Perlindungan Hukum di Indonesia*, CV. Adanu Abimata, Indramayu, 2026.
- A.P.A. Santoso et al, *Kapita Selekta Hukum Pidana. Suatu Pengenalan Dasar*, Pustakabarupress, Yogyakarta, 2022.
- Danvrianto Budhijanto, *Hukum Perlindungan Data Pribadi di Indonesia (Cyberlaw & Cybersecurity)*, PT Refika Aditama, Bandung, 2023.
- Filep Wamafma, dkk, *Perlindungan Hukum bagi Konsumen dalam Transaksi E-commerce*, Penerbit Amerta Media, Purwokerto, 2023.
- I Gusti Kade Budhi, *Artificial Intelligence : Konsep, Potensi Masalah, Hingga Pertanggungjawaban Pidana*, PT RajaGrafindo Persada, Depok, 2022.
- Ika Menarianti, dkk, *E-Commerce*, CV. Eureka Media Aksara, Purbalingga, 2024.
- Ismail Koto & di Faisal, *Buku Ajar Hukum Perlindungan Saksi dan Korban*, Umsu Press, Medan, 2022.



- Lexy J. Moleong, *Metodologi Penelitian Kualitatif (Edisi Revisi)*, Remaja Rosdakarya, Bandung, 2021.
- Mod. Yusuf Daeng, Siti Yulia Makkininnawa, M. Fadly Daeng Yusuf, *Hukum Perlindungan Konsumen*, Taman Karya, Pekanbaru, 2024.
- Mohammad Adrin Akbar dan Sitti Nur Alam, *E-Commerce Dasar Teori Dalam Bisnis Digital*, Yayasan Kita Menulis, Jakarta, 2020,
- Muhaimin, *Metode Penelitian Hukum*, Mataram University Press, Mataram, 2020.
- Rizky P.P Karo Karo, dkk. *Pengaturan Perlindungan Data Pribadi di Indonesia*, Nusa Media, Bandung, 2020.
- Sinta Dwi Rosadi, *Pembahasan UU Perlindungan Data Pribadi (UU RI No.27 Tahun 2022)*, Sinar Grafika, Jakarta, 2023.
- Soerjono Soekanto & Sri Mamudji, *Penelitian Hukum Normatif (Suatu Tinjauan Singkat) Cetakan Ke 22*, PT RajaGrafindo Persada, Jakarta, 2024.
- Sri Rizqi Wahyuningrum, *Statistika Pendidikan*, Deepublish, Yogyakarta, 2020.
- Sugeng, *Hukum Telematika Indonesia*, Prenadamedia Group, Jakarta, 2020.
- Sugiyono, *Metode Penelitian Kuantitatif, Kualitatif, dan R&D*, Alfabeta, Bandung, 2022.
- Tomi Wicaksono Putra, Hamidah Abdurrachman, dan Achmad Irwan Hamzani, *Pertanggungjawaban Pidana Terhadap Kejahatan Hacking*, PT Nasya Expanding Management, Pekalongan, 2023.

PERATURAN PERUNDANG-UNDANGAN :

- Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.
- Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi
- Undang-Undang Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen
- Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik

JURNAL :

- Audrey Bilbina Putri, Jocelyn Cherieshta, dan Rasji, “Penguraian Konsep Tanggung Jawab dalam Filsafat Hukum: Dari Dimensi Individu ke Masyarakat,” *Jurnal Ilmiah Wahana Pendidikan*, Vol. 10, No. 8, 2024.
- Dika Ratu Marfu’atun, “Perlindungan Konsumen terhadap Penggunaan Klausula Baku tentang Pemberian Kuasa dalam Perjanjian Kredit Bank di PT Bank Pembangunan Daerah Jawa Barat dan Banten Tbk Kantor Cabang Khusus Banten”, *Nurani Hukum: Jurnal Ilmu Hukum*, Vol. 3, No.1. 2020.
- Febrian Hilmi Firdaus, “Perlindungan dan Kepastian Hukum bagi Pengendali Data Pribadi di Masa Depan”, *Masalah-Masalah Hukum*, Vol. 53 No. 2, 2024.
- Febrika Patricia Carolin Mamadoa, Herlyanty Y. A. & Bawole Yumi Simbala, “Larangan Dan Sanksi Atas Perolehan Dan Penggunaan Data Pribadi Secara Melawan Hukum Berdasarkan UU No 27 Tahun 2022 Tentang Perlindungan Data Pribadi”, *Jurnal Fakultas Hukum Unsrat*, Vol. 15, No. 3, 2026.
- Hendra Saputra, dkk. “Analisis Tanggung Jawab Etis dan Hukum Perusahaan E-Commerce terhadap Perlindungan Data Pribadi Konsumen: Studi Kasus Kebocoran Data Tokopedia 2020”, *SCIENTIFIC JOURNAL OF REFLECTIO : Economic, Accounting, Management and Business*, Vol. 9, No. 1, January 2026.
- Hetty Hasaanah & Wahyudi, “Legal Protection of Cosumer Personal Data on the Use of Fintech in E-commerce” *Jurnal Bina Mulia Hukum*, Vol. 10, No. 1, 2025, hlm.74.



- Jumriani, “*Cash On Delivery (COD) Perspektif Ekonomi Syari’ah*” *Journal of Environmental Economics and Sustainability*, Volume: 1, Nomor 2, 2024.
- Jureid, “*Cash on Delivery sebagai Pengaruh Minat Belanja Online di E-Commerce*,” *Profetik Jurnal Ekonomi Syariah*, Vol. 3 No. 2, 2024.
- Mahisa Mareati, dkk., “*Analisis Hukum Perlindungan Data Pribadi pada Platform E-Commerce di Era Digital*,” *Al-Zayn: Jurnal Ilmu Sosial & Hukum*, Vol. 2, No. 1, 2025.
- Predderics Hockop Simanjuntak, “*Perlindungan Hukum terhadap Data Pribadi pada Era Digital di Indonesia*,” *Jurnal Esensi Hukum*, Vol. 6 No. 2, 2024.
- Rahmansyah Fadlul Al Karim Rambe, dkk., “*Implikasi Perlindungan Hak Asasi Manusia dalam Hukum Pidana*,” *Jurnal Ilmiah Penegakan Hukum*, Vol. 11 No. 1, 2024.
- Robby Nurtresna, “*Tinjauan Yuridis Perlindungan Hukum Bagi Konsumen Jasa Pengobatan Tradisional*,” *DESANTA Indonesian Of Interdisciplinary Journal*, Vol. 2, No. 2, 2022.
- Robby Nurtresna, “*Legal Analysis of Digital Trade in Indonesia Based on Law Number 11 of 2008 concerning Electronic Information and Transactions*,” *Fox Justi: Jurnal Ilmu Hukum*, Vol. 15, No. 2, 2025.
- Tengku Mega Rahmadini, “*Pertanggungjawaban Perdata Atas Penyalahgunaan Data Pribadi Konsumen dalam Transaksi Elektronik di Indonesia*,” *Al-Zayn : Jurnal Ilmu Sosial & Hukum*, Vol. 4, No. 2, 2026.

WEBSITE :

- ADCO Law, “*Perlindungan Hukum Bagi Masyarakat*” 2022, <https://adcolaw.com/id/blog/perlindungan-hukum-bagi-masyarakat/>. Diakses Pada Hari Senin, 08 Juni 2026, Pukul 08.02 Wib.
- Detik.com, “*Kemendagri Ingatkan Fotokopi E-KTP Langgar Perlindungan Data Pribadi*.” <https://www.detik.com/jogja/berita/d-8477704/kemendagri-ingatkan-fotokopi-e-ktp-langgar-perlindungan-data-pribadi>. Diakses Pada Hari Sabtu, 30 Mei 2026 Pukul 14.04 Wib.
- Julie Young, “*Cash on Delivery (COD): What It Is and How It Works*,” *Investopedia*, 2024, Diakses Melalui <https://www.investopedia.com/terms/c/cashondelivery.asp>. Pada hari Minggu, 07 Juni 2026. Pukul 09.48 Wib
- Kholida Qothrunnada, “*Cash On Delivery (COD): Pengertian, Cara Kerja, Dan Tipsnya*,” *Finance.detik*, 2022, Diakses Melalui <https://finance.detik.com/berita-ekonomi-bisnis/d-5971563/cash-on-delivery->. Diakses Pada hari Minggu, 07 Juni 2026. Pukul 08.12 Wib
- Nur Rachmi Latifa, “*Faktor Penyebab Kebocoran Data dan Cara Mengatasinya*” . Diakses Melalui <https://sibermate.com/id/hrmi/faktor-penyebab-kebocoran-data-dan-cara-mengatasinya> Pada Hari Sabtu, 30 Mei 2026. Pukul 13.45 Wib.
- Pandi Apriyandi, “*15+ Kelebihan dan Kekurangan COD bagi Penjual & Pembeli*”, 2025, Diakses Melalui <https://share.google/oCobeAxmQvHPxRIQI> Pada Hari Selasa, 28 Juli 2026. Pukul 14.23 wib.