

PERLINDUNGAN DATA PRIBADI DALAM TRANSAKSI ELEKTRONIK MENURUT HUKUM PERDATA DALAM PENGGUNA TRANSPORTASI DARING

Oleh:

Anne Joyce Lauren Sirumapea¹

Dewa Ayu Dian Sawitri²

Universitas Udayana

Alamat: JL. Pulau Bali No. 1, Dauh Puri Klod, Kec. Denpasar Barat, Kota Denpasar,
Bali (80114).

Korespondensi Penulis: annejoycel Lauren@gmail.com,
dewaayudiansawitri@unud.ac.id.

Abstract. *The phenomenon of information technology disruption has now driven the development of ride-hailing services as part of the sharing economy in modern urban society. Behind the benefits offered, these services carry serious vulnerabilities regarding the protection of users' digital personal data. Information such as names, addresses, phone numbers, and geolocation can be accessed by both the platform providers and drivers, and has the potential to be misused for purposes beyond transportation services. This study aims to examine the legal protection of digital personal data of ride-hailing users in Indonesia and to assess the responsibility of platform providers and third parties in the context of privacy protection. Using a normative approach to the applicable regulations, this research finds that legal protection remains weak due to regulatory gaps, standard clauses that disadvantage consumers, and the storage of data outside Indonesia's jurisdiction that is difficult to monitor. In conclusion, specific regulations and more comprehensive legal mechanisms are needed to effectively safeguard the digital privacy rights of ride-hailing users in the current digital era.*

Keywords: Legal Protection, Personal Data, Ride-Hailing Services, Digital Privacy.

PERLINDUNGAN DATA PRIBADI DALAM TRANSAKSI ELEKTRONIK MENURUT HUKUM PERDATA DALAM PENGGUNA TRANSPORTASI DARING

Abstrak. Fenomena disrupsi teknologi informasi kini telah mendorong perkembangan transportasi daring sebagai bagian dari *sharing economy* di masyarakat urban modern. Di balik manfaat yang ditawarkan, layanan ini menyimpan kerentanan yang cukup serius terkait perlindungan data pribadi digital pengguna. Informasi seperti nama, alamat, nomor telepon, hingga geolokasi dapat diakses oleh aplikator maupun driver, dan dapat berpotensi disalahgunakan untuk kepentingan di luar layanan transportasi. Penelitian ini bertujuan untuk mengkaji bentuk perlindungan hukum terhadap data pribadi digital pengguna transportasi daring di Indonesia serta menilai tanggung jawab pihak aplikator maupun pihak ketiga dalam konteks perlindungan privasi. Dengan menggunakan pendekatan normatif terhadap peraturan yang berlaku, penelitian ini menemukan bahwa perlindungan hukum masih lemah akibat kekosongan regulasi, klausula baku yang merugikan konsumen, serta penyimpanan data di luar yurisdiksi Indonesia yang sulit diawasi. Hasil dari penelitian ini menjelaskan bahwa dibutuhkan regulasi khusus dan mekanisme hukum yang lebih komprehensif agar hak privasi digital pengguna transportasi daring dapat terlindungi secara efektif dalam era digital saat ini.

Kata Kunci: Perlindungan Hukum, Data Pribadi, Transportasi Daring, Privasi Digital.

LATAR BELAKANG

Dalam lima tahun terakhir, fenomena disrupsi teknologi informasi mendorong perkembangan *sharing economy*, salah satunya di sektor transportasi daring (Go-Jek, Grab, Uber)¹. Data November 2017 menunjukkan Go-Jek memiliki 8,8 juta pengguna, Grab 8,6 juta. Pengguna urban lebih memilih transportasi daring karena praktis, aman, cepat, dan tanpa tawar-menawar. Bagi driver, transportasi daring menarik karena fleksibilitas, kompensasi, dan penghasilan yang sebanding dengan pekerjaan sebelumnya.²

Konsep *sharing economy* dalam transportasi daring diminati karena tiga faktor³:

1. *Economical drivers* – pasca krisis 2008, masyarakat mencari alternatif bisnis dengan modal kecil dan sistem berbagi aset.

¹ Sulaiman, King Faisal. Teori dan Hukum Konstitusi (Bandung, Nusa Media, 2019), 132

² Muhammad Taufik Ajiputera and Heru Susetyo. (2024). Implementasi Pengaturan Hak Untuk Dilupakan Melalui Sistem Penghapusan Data Pribadi Dan/Atau Dokumen Elektronik Menurut Perspektif Hukum Positif Di Indonesia. *Unes Law Review*, 6(3): 8051–67, p. 8052.

³ Syamsudin, Rahman. Pengantar Hukum Indonesia (Jakarta, Kencana, 2019), 199

2. *Societal drivers* – urbanisasi meningkat pesat tanpa seimbangnya lapangan kerja, sehingga transportasi daring jadi solusi ekonomi masyarakat bawah.
3. *Technological drivers* – kemajuan teknologi internet mendukung pencarian konsumen secara efisien.

Namun, muncul pula persoalan seperti izin trayek, persaingan dengan transportasi konvensional, hingga isu privasi data pengguna (nama, email, nomor telepon, alamat, rute perjalanan) yang dapat diakses driver dan aplikator. Data pribadi ini bernilai ekonomi dan menjadi bagian dari digital dossier.⁴

Selain transportasi daring, perkembangan e-commerce juga pesat. Contoh: Bukalapak dengan 35 juta pengguna aktif bulanan dan 320 ribu transaksi per hari, berkembang berkat promosi media sosial, fitur mudah, dan sistem transaksi praktis. Secara keseluruhan, ekonomi digital memberikan banyak manfaat: pilihan produk beragam, efisiensi waktu, serta kemudahan transaksi, meski tetap menyimpan tantangan dalam aspek regulasi dan perlindungan data pribadi.⁵ Pengumpulan data pribadi digital seseorang dapat dikumpulkan dari aplikasi transportasi daring.⁶

Penggunaan aplikasi transportasi daring tentunya calon pengguna diharuskan untuk mendaftar dan memberikan data-data pribadi mereka kepada aplikator serta akan disimpan dalam *Big Data* milik aplikator. Namun pengumpulan data-data privasi dan penggunaan aplikasi internet akan meninggalkan jejak digital serta menimbulkan kekhawatiran tentang sebuah dunia tanpa privasi dan perusahaan aplikator menjadi lebih mengetahui tentang diri kita.⁷

Apabila penggunaan data-data privasi konsumen dalam cara yang bertanggungjawab, penuh rasa saling menghormati, dan sesuai konteks tujuan, maka pengumpulan data privasi konsumen dapat membantu individu dan institusi untuk membuat keputusan lebih baik. Namun apabila pengumpulan data privasi konsumen

⁴ Erlyns Yolanda and Rugun Romaida Hutabarat.(2023). Urgensi lembaga perlindungan data pribadi di Indonesia berdasarkan asas hukum responsif. *Syntax Literate: Jurnal Ilmiah Indonesia*, 8(6) p. 4175.

⁵ Sinta Dewi Rosadi, Konsep Perlindungan Hukum Atas Privasi dan Data Pribadi Dikaitkan dengan Penggunaan *Cloud Computing* di Indonesia, *Yustisia Jurnal Hukum*, Vol. 5, No. 1 (2016), hlm. 23

⁶ Parihin, Nela mardiana. 2023. “Urgensi Perlindungan Data Pribadi Dalam Perpektif Hak Asasi Manusia”. *Jurnal Rechten : Riset Hukum Dan Hak Asasi Manusia* 5 (1), 16-23. <https://doi.org/10.52005/rechten.v5i1.108>.

⁷ Kukuh Tejomurti, The Personal Electronic Data Security on The Implementation of Solo Smart City According to The Perspective of Privacy Protection Law, *Journal of Law, Policy, and Globalization*, Vol. 66 (2017). Hlm 1

PERLINDUNGAN DATA PRIBADI DALAM TRANSAKSI ELEKTRONIK MENURUT HUKUM PERDATA DALAM PENGGUNA TRANSPORTASI DARING

digunakan tidak sesuai dengan konteks tujuan awal, maka pelanggaran hak atas privasi akan terjadi. Pembukaan informasi-informasi yang bersifat rahasia merupakan tujuan dibentuknya *big data*. Perilaku konsumen dalam aktivitas sosial, politik, dan orientasi seksual menjadi sebuah isu menarik bagi perusahaan penyedia jasa aplikasi daring.

Pertanyaan esensial muncul mengenai keamanan perlindungan data privasi pengguna transportasi daring di masyarakat urban yang cenderung terbuka dan mudah memberi data privasi mereka pada aplikasi transportasi daring. Data privasi seperti: Nama, E-mail dan Nomor *handphone* pengguna akan tersimpan otomatis pada aplikator dan pihak ketiga seperti *driver*. Apabila *handphone* masing-masing pengguna dan *driver* memiliki aplikasi *whatsapp* atau *Line*, maka akun *whatsapp* dan nama pengguna secara otomatis akan tersimpan di *handphone* pihak ketiga seperti *driver* atau pihak lain apabila berkepentingan terhadap data privasi pengguna tersebut.

Deklarasi Universal Hak Asasi Manusia (DUHAM) Perserikatan Bangsa-Bangsa ditegaskan bahwa tidak seorang pun boleh diganggu secara sewenang-wenang dalam urusan privasinya, keluarganya, rumah tangganya, maupun surat-menyuratnya, serta tidak boleh diserang kehormatan dan reputasinya. Setiap orang berhak memperoleh perlindungan hukum terhadap gangguan atau serangan semacam itu. Hal ini sejalan dengan Pasal 28G Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 yang menyatakan bahwa setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda di bawah kekuasaannya, serta berhak memperoleh rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasinya.⁸

Dalam penelitian yang diterbitkan pada September 2023 oleh Yunas dan Nasution, yang berjudul “Perlindungan Hukum terhadap Privasi Data Pribadi Konsumen Pengguna Gojek di Indonesia”, yang dipublikasikan dalam jurnal SAMMAJIVA: Jurnal Penelitian Bisnis dan Manajemen (Vol. 1, No. 3), topik penelitian yang dikaji ini jika dibandingkan dengan penelitian tersebut sama-sama berkenaan dengan tema perlindungan hukum terhadap privasi data pribadi pengguna transportasi daring di Indonesia melalui kajian yuridis normatif. Tujuan utama dari penelitian tersebut adalah

⁸ Ahmad Budi Setiawan.(2018). Revolusi Bisnis Berbasis Platform Sebagai Penggerak Ekonomi Digital Di Indonesia. Masyarakat Telematika Dan Informasi : Jurnal Penelitian Teknologi Informasi Dan Komunikasi, 9(1): 56-75 DOI 10.17933/mti.v9i1.118, p. 61

menganalisis bagaimana perusahaan Gojek bertanggung jawab dan menerapkan kebijakan privasi data pengguna di tengah perkembangan teknologi digital, khususnya dalam kerangka hukum Indonesia. Penelitian ini menyoroti bahwa perlindungan data pribadi sangat bergantung pada peraturan yang ada dan mengungkap kerentanan nyata dalam sistem Gojek, terutama potensi penyalahgunaan data oleh driver yang dapat memicu teror terhadap konsumen. Pada aplikasi online seperti gojek, ancaman keprivasian dapat terlihat dari mudahnya driver dalam mengetahui alamat serta nomor telepon pribadi pengguna Gojek. Sehingga penting bagi perusahaan ini memperhatikan aspek perlindungan data pribadi konsumennya.⁹

Rumusan Masalah

Berdasarkan hal tersebut, rumusan masalah dalam penelitian ini adalah

1. bagaimana bentuk perlindungan hukum terhadap data pribadi digital pengguna transportasi daring di Indonesia?
2. Bagaimana pertanggungjawaban pihak ketiga apabila terjadi kegagalan perlindungan data?

Tujuan Penelitian

Penelitian ini bertujuan untuk

1. Mengkaji dan menganalisis bentuk perlindungan hukum terhadap data pribadi digital pengguna transportasi daring di Indonesia
2. Mengkaji dan menganalisis pertanggungjawaban pihak ketiga apabila terjadi kegagalan perlindungan data.

METODE PENELITIAN

Penelitian ini menggunakan metode penelitian hukum normatif¹⁰. Pendekatan normatif dilakukan melalui telaah peraturan perundang-undangan yang relevan, antara lain UUD 1945, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik beserta perubahannya, Peraturan Pemerintah Nomor 82 Tahun 2012 tentang

⁹ Hesty Ananta Yunas dan Muhammad Irwan Padli Nasution. (2023). Perlindungan Hukum Terhadap Privasi Data Pribadi Konsumen Pengguna Gojek di Indonesia. *SAMMAJIVA: Jurnal Penelitian Bisnis dan Manajemen* Vol. 1, No. 3: 69-73.

¹⁰ Marzuki, Peter Mahmud. *Penelitian Hukum* (Jakarta, Kencana, 2017), 97

PERLINDUNGAN DATA PRIBADI DALAM TRANSAKSI ELEKTRONIK MENURUT HUKUM PERDATA DALAM PENGGUNA TRANSPORTASI DARING

Penyelenggaraan Sistem dan Transaksi Elektronik, serta Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik.

HASIL DAN PEMBAHASAN

Bentuk Perlindungan Hukum Terhadap Data Pribadi Digital Pengguna Transportasi Daring di Indonesia

Perlindungan atas data pribadi kini diakui sebagai bagian penting dari hak asasi manusia. Hal ini mendorong banyak negara untuk menetapkan perlindungan data sebagai hak konstitusional atau yang dikenal dengan istilah “habeas data”, yaitu hak individu untuk mendapatkan jaminan keamanan atas data pribadinya serta hak untuk mengoreksi jika terdapat kesalahan dalam data tersebut. Portugal merupakan salah satu negara yang memasukkan perlindungan data dalam konstitusinya. Deklarasi Hak Asasi Manusia ASEAN juga memuat pengakuan terhadap hak atas privasi. Saat ini, tercatat lebih dari 75 negara telah mengatur perlindungan data dalam sistem hukum atau peraturan perundang-undangannya masing-masing. Perlindungan data pribadi di Argentina termasuk sebagai bagiannya¹¹, Hukum di Kanada yang mengatur perlindungan informasi pribadi serta dokumen elektronik, Sejumlah ketentuan hukum, termasuk Undang-Undang Perlindungan Data Pribadi di Jepang, Peraturan Teknologi Informasi di India, Undang-Undang Perlindungan Informasi Pribadi di Korea Selatan, Undang-Undang Perlindungan Data di Singapura, dan Undang-Undang Data Pribadi di Filipina, pada umumnya berlandaskan prinsip-prinsip Organization for Economic Co-Operation and Development (OECD) serta banyak yang mendapat pengaruh dari regulasi Uni Eropa.¹²

Di Uni Eropa, perlindungan data dan privasi bagi seluruh individu di kawasan Eropa serta Wilayah Ekonomi Eropa diatur melalui General Data Protection Regulation (GDPR). Regulasi ini bertujuan memberikan kendali yang lebih besar kepada warga negara dan penduduk Uni Eropa atas data pribadi mereka sekaligus menyederhanakan aturan bagi perusahaan internasional. Setiap perusahaan diwajibkan menerapkan standar

¹¹ Ahmad Rayhan and others.(2024). Evektifitas Hukum Sistem Pembuktian Alat Bukti Elektronik Dalam Ranah Pemeriksaan Bukti Di Pengadilan Tata Usaha Negara. Jurnal Res Justitia: Jurnal Ilmu Hukum, 4(1): 279–95, p. 285.

¹² Daniel J. Solove, 2017, *A Brief History of Information Privacy Law*, George Washington University Law School Public Law Research Paper No. 215

yang lebih tinggi dalam menjaga keamanan data. Pelanggaran terhadap GDPR dapat berakibat sanksi hingga 20 juta Euro. Dampak regulasi ini juga dirasakan India. Pada tahun 2010, India belum memiliki standar yang memadai terkait keamanan dan privasi data sehingga ekspor data pribadi dari negara-negara anggota Uni Eropa ke India dibatasi. Sebagai tindak lanjut, India dan Uni Eropa membentuk Kelompok Ahli bersama untuk merumuskan sistem perlindungan data yang lebih memadai.¹³

Terkait dengan data privasi, Ann Covoukian menyatakan bahwa privasi merupakan hak seseorang untuk mengendalikan informasi pribadinya serta memiliki kewenangan menentukan sejauh mana dan dengan cara apa informasi tersebut dikumpulkan maupun digunakan.¹⁴

Privasi sebagai bagian dari hak asasi manusia setidaknya mencakup tiga unsur utama. Pertama, privasi mengenai diri seseorang yang berlandaskan pada prinsip umum *the right to be alone*, yakni hak setiap individu untuk dibiarkan sendiri tanpa gangguan pihak lain. Dalam aspek ini, terdapat beberapa bentuk pelanggaran yang dapat terjadi, seperti menampilkan seseorang dalam konteks yang keliru atau tidak tepat, misalnya penggunaan foto seseorang pada ilustrasi kasus kekerasan dalam rumah tangga tanpa persetujuan—hingga pengungkapan identitas atau hobi pribadi seseorang di ruang publik untuk kepentingan komersial.

Selain itu, penyebaran informasi pribadi yang bersifat memalukan kepada masyarakat luas maupun tindakan yang mengganggu hak seseorang untuk menikmati kesendirian juga termasuk bentuk pelanggaran privasi personal. Kedua, privasi data pribadi (*privacy of data about person*) yang merujuk pada hak seseorang untuk mengendalikan informasi yang berkaitan dengan dirinya, baik yang dikumpulkan maupun digunakan oleh pihak lain. Data tersebut dapat berupa catatan medis, kebiasaan hidup, keanggotaan organisasi politik, data perpajakan, asuransi, hingga catatan pidana.

Penyalahgunaan data yang dihimpun dari konsumen atau masyarakat bukan hanya merugikan secara material, tetapi juga melanggar hak dasar atas privasi. Ketiga, privasi komunikasi yang menyangkut interaksi seseorang, khususnya di ruang digital. Dalam konteks ini, tindakan pengawasan, penyadapan, maupun pembocoran isi komunikasi

¹³ Fikri and Rusdiana.(2023). Ruang Lingkup Perlindungan Data Pribadi: Kajian Hukum Positif Indonesia. Ganesha Law Review, 5(1): p. 51.

¹⁴ Ramli, Ahmad M., Tasya Safiranita Ramli, and Ferry Gunawan. *Hukum Telematika*. 2nd ed. Tangerang Selatan: Universitas Terbuka, 2020. hlm. 163.

PERLINDUNGAN DATA PRIBADI DALAM TRANSAKSI ELEKTRONIK MENURUT HUKUM PERDATA DALAM PENGGUNA TRANSPORTASI DARING

elektronik oleh pihak yang tidak berwenang dapat dikategorikan sebagai pelanggaran hak privasi, karena komunikasi seharusnya hanya menjadi domain antara pengirim dan penerima yang sah. Dengan demikian, ketiga unsur tersebut menegaskan bahwa privasi tidak hanya terkait dengan ruang pribadi seseorang, tetapi juga mencakup data serta komunikasi yang harus dilindungi demi menjamin penghormatan terhadap martabat manusia.¹⁵

Secara historis, hak privasi memiliki cakupan luas dalam perspektif antropologis dan sosiologis. Alan Westin mengemukakan bahwa hak privasi merupakan tuntutan individu dan kelompok untuk menentukan sendiri bagaimana, apa, dan kapan informasi tentang mereka dibagikan kepada publik¹⁶ Menurut William G. Staples, hak privasi memiliki fungsi melindungi individu maupun kelompok dari kemungkinan atau risiko terluka secara emosional akibat pihak lain mengetahui fakta yang benar tetapi bersifat memalukan tentang mereka. Di sisi lain, Mahkamah Agung Amerika Serikat melalui putusan-putusan yudisialnya menegaskan bahwa terdapat dua unsur pokok dalam hak privasi:¹⁷

1. Hak individu untuk menjaga agar informasi pribadinya tidak dipublikasikan kepada publik.
2. Hak individu untuk bebas menentukan berbagai keputusan tertentu dalam hidupnya.

Dalam konteks perlindungan hak asasi manusia di tingkat internasional, hak atas privasi memperoleh jaminan melalui Pasal 12 Deklarasi Umum Hak Asasi Manusia (DUHAM) yang menegaskan bahwa tidak seorang pun boleh diganggu secara sewenang-wenang dalam urusan privasi, keluarga, rumah, maupun korespondensinya, serta tidak boleh diserang kehormatan dan reputasinya, dan setiap orang berhak atas perlindungan hukum terhadap gangguan atau serangan semacam itu. Jaminan serupa juga ditegaskan dalam Pasal 17 Kovenan Internasional tentang Hak-Hak Sipil dan Politik yang menyatakan, pertama, bahwa tidak seorang pun boleh secara sewenang-wenang maupun melawan hukum dicampuri urusan pribadinya, keluarganya, tempat tinggalnya, atau komunikasi surat-menyuratnya, serta tidak boleh diserang secara tidak sah kehormatan

¹⁵ *Ibid.*, hlm. 160

¹⁶ *Ibid*

¹⁷ N. A. Moreham and Adam Speker, eds. *The Law of Privacy and the Media*. 4th ed. Oxford: Oxford Law Pro, 2024. hlm. 397-398

dan reputasinya, dan kedua, bahwa setiap individu berhak memperoleh perlindungan hukum terhadap campur tangan atau serangan tersebut.

Dalam hukum nasional, Pasal 28G ayat (1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 juga secara tegas menyatakan bahwa setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang berada di bawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi manusia.

Berdasarkan Pasal 28G ayat (1) UUD 1945, dapat dipahami bahwa setiap warga negara Indonesia memiliki hak atas privasi data pribadi (privacy of data about person), yaitu hak yang melekat pada informasi individu yang dikumpulkan dan digunakan oleh pihak lain. Pengabaian terhadap hak privasi data pribadi tersebut berpotensi menimbulkan pelanggaran terhadap hak-hak konstitusional warga negara.

Pertanggungjawaban Pihak Ketiga Apabila Terjadi Kegagalan Perlindungan Data

Perkembangan teknologi internet tidak selalu beriringan dengan penguatan perlindungan hak privasi individu maupun kelompok. Justru, privasi seseorang menjadi semakin rentan terhadap intervensi dan data pribadi kian mudah dialihkan. Salah satu bentuk kerentanan dalam pemindahan data pribadi terlihat pada hadirnya layanan transportasi daring berbasis aplikasi, di mana pengguna atau konsumen diminta memberikan informasi pribadinya seperti nama, alamat, tanggal lahir, email, pekerjaan, hingga lokasi rumah dan kantor (terutama bagi pengguna yang bekerja sebagai karyawan).

Berdasarkan dua kebijakan privasi transportasi daring tersebut dapat dipahami bahwa:

1. Perusahaan aplikator transportasi daring mengumpulkan data pribadi pelanggan maupun mitra pengemudi dalam bentuk big data yang dimiliki perusahaan.
2. Setelah transaksi selesai, pihak ketiga (penyedia layanan/driver) berpotensi menyimpan data pribadi pelanggan dengan berbagai cara. Pada aplikasi Gojek secara khusus disebutkan bahwa aplikator tidak bertanggung jawab atas tindakan pihak penyedia layanan/driver, dan pelanggan dianggap setuju untuk membela, tidak menuntut ganti rugi, serta membebaskan aplikator dari tanggung jawab tersebut.

PERLINDUNGAN DATA PRIBADI DALAM TRANSAKSI ELEKTRONIK MENURUT HUKUM PERDATA DALAM PENGGUNA TRANSPORTASI DARING

3. Data pribadi pelanggan dapat dipindahkan, disimpan, digunakan, dan diproses di yurisdiksi lain di luar Indonesia tempat server perusahaan aplikasi berada.
4. Pada aplikasi Grab Group, data pribadi pelanggan dapat dialihkan, dinilai, atau dibagikan kepada pihak ketiga baik di dalam maupun luar negeri untuk berbagai tujuan utama dan tambahan.
5. Terkait hukum, yurisdiksi, dan penyelesaian sengketa:
 - a. Aplikasi Gojek menunjuk Pengadilan Negeri Jakarta Selatan sebagai forum penyelesaian sengketa.
 - b. Aplikasi Grab tidak menentukan secara khusus pengadilan atau lembaga yang berwenang menyelesaikan sengketa.

Berdasarkan rumusan masalah tersebut, dapat dianalisis bahwa pelanggan aplikasi transportasi daring menyerahkan berbagai data pribadi seperti nama, foto, alamat rumah, lokasi, tempat kerja, dan ID pengguna. Keterbukaan data ini membuat aktivitas pelanggan dapat dipetakan, misalnya jadwal berangkat dan pulang kerja, rute perjalanan sehari-hari, hingga kondisi rumah dan kantor. Informasi tersebut rawan dimanfaatkan pihak yang tidak bertanggung jawab untuk melakukan tindak kriminal, mulai dari perampokan, pelecehan, hingga penjualan data ke pihak lain. Saat ini belum ada aturan khusus yang secara komprehensif mengatur tata kelola perlindungan data pribadi digital pengguna transportasi daring.

Kerentanan privasi juga terjadi karena pihak aplikasi memiliki akses atas preferensi penggunaan fitur aplikasi, sementara penyedia layanan atau pengemudi dapat dengan mudah mengakses data pribadi seperti geolokasi rumah, tempat kerja, serta nomor telepon yang terhubung ke aplikasi pesan instan seperti WhatsApp atau Line. Kondisi ini membuka celah pemanfaatan data pribadi di luar tujuan layanan transportasi tanpa izin pemilik data. Padahal, Pasal 26 UU No. 11 Tahun 2008 tentang ITE dan Pasal 21 Permenkominfo No. 20 Tahun 2016 dengan jelas menyatakan bahwa penggunaan dan penyebaran data pribadi dalam sistem elektronik hanya boleh dilakukan dengan persetujuan pemilik data. Artinya, meskipun pengguna telah menyetujui kebijakan privasi saat mendaftar aplikasi, persetujuan itu hanya mengikat dengan aplikasi sebagai penyelenggara sistem, bukan pihak ketiga seperti pengemudi, perusahaan pemasaran, sponsor, maupun periklanan.

Pihak yang bertanggung jawab atas kegagalan perlindungan dan kebocoran data, Pasal 15 Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE) menetapkan bahwa:

“Apabila terjadi kegagalan dalam perlindungan data pribadi yang dikelola, Penyelenggara Sistem Elektronik wajib menyampaikan pemberitahuan secara tertulis kepada pemilik data pribadi.”

Istilah “kegagalan” dalam Pasal 15 PP PSTE tidak diberikan definisi secara spesifik. Namun, Pasal 15 ayat (1) UU ITE menjelaskan bahwa kegagalan dapat berupa kegagalan prosedural terkait kerahasiaan dan keamanan dalam pengolahan data, serta kegagalan sistem dari sisi keandalan dan keamanan sistem yang digunakan. Menurut penulis, apabila pihak ketiga (penyedia layanan/driver) dapat mengakses dan memanfaatkan data pribadi pengguna tanpa persetujuan, hal ini dapat dikategorikan sebagai kegagalan prosedural dalam menjaga kerahasiaan dan keamanan data, sehingga aplikator sebagai penyelenggara sistem elektronik bertanggung jawab atas risiko pelanggaran hak privasi pengguna.

Data pribadi pengguna aplikasi dapat disimpan, diolah, dan dialihkan ke server yang berada di luar yurisdiksi Indonesia. Penggunaan aplikasi transportasi daring memiliki potensi risiko penyalahgunaan informasi pribadi. Kebijakan privasi dari dua perusahaan transportasi daring menunjukkan bahwa data pengguna dapat digunakan, diproses, dan dipindahkan ke server di luar wilayah hukum Indonesia. Hal ini menimbulkan persoalan kompleks jika terjadi penyalahgunaan data, karena menyangkut perbedaan yurisdiksi hukum dan variasi regulasi perlindungan data antarnegara, terutama di negara yang memberikan kebebasan bagi perusahaan swasta untuk mengatur pengolahan data mereka sendiri.

Pengguna aplikasi yang mengalami kerugian akibat tindakan ilegal pihak ketiga (penyedia layanan/driver) dapat memanfaatkan alat bukti elektronik untuk mengajukan gugatan ganti rugi atas kerugian yang timbul akibat kegagalan perlindungan keamanan data pribadi. Namun, konsumen menghadapi kendala karena kebijakan privasi umumnya menetapkan secara standar bahwa aplikator tidak bertanggung jawab atau mengalihkan tanggung jawabnya kepada pihak lain apabila pihak ketiga (driver atau pihak lain) menggunakan data pribadi pengguna tanpa izin pemilik data. Sesuai Pasal 18 Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen, disebutkan bahwa:

PERLINDUNGAN DATA PRIBADI DALAM TRANSAKSI ELEKTRONIK MENURUT HUKUM PERDATA DALAM PENGGUNA TRANSPORTASI DARING

“Pelaku usaha yang menawarkan barang dan/atau jasa untuk diperdagangkan dilarang menyertakan klausula baku dalam setiap dokumen atau perjanjian apabila klausula tersebut menyatakan pengalihan tanggung jawab pelaku usaha, ... dan ketentuan lainnya”

Dalam hal ini, muncul kekhawatiran terkait kontrak standar karena adanya klausula eksonerasi, yaitu klausula yang memuat ketentuan yang membatasi atau bahkan menghapus sepenuhnya tanggung jawab yang seharusnya ditanggung oleh pihak penyedia (penyelenggara sistem elektronik).

KESIMPULAN DAN SARAN

Penelitian ini menyimpulkan bahwa perlindungan data pribadi pengguna transportasi daring di Indonesia masih lemah. Meskipun telah ada dasar normatif dalam UUD 1945, UU ITE, PP PSTE, dan Permenkominfo No. 20 Tahun 2016, namun regulasi tersebut belum secara khusus mengatur tata kelola data pribadi pada layanan transportasi daring. Aplikator cenderung melepaskan tanggung jawab dengan klausula baku, sementara driver memiliki akses langsung pada data pribadi pengguna yang rawan disalahgunakan. Selain itu, data pengguna juga dapat diproses dan disimpan di luar yurisdiksi Indonesia, sehingga menambah kompleksitas perlindungan hukum.

DAFTAR REFERENSI

Buku

- Marzuki, Peter Mahmud. *Penelitian Hukum*. Jakarta: Kencana, 2017.
- Moreham, N. A., and Adam Speker, eds. *The Law of Privacy and the Media*. 4th ed. Oxford: Oxford Law Pro, 2024.
- Ramli, Ahmad M., Tasya Safiranita Ramli, and Ferry Gunawan. *Hukum Telematika*. 2nd ed. Tangerang Selatan: Universitas Terbuka, 2020.
- Sulaiman, King Faisal. *Teori dan Hukum Konstitusi*. Bandung: Nusa Media, 2019.
- Syamsudin, Rahman. *Pengantar Hukum Indonesia*. Jakarta: Kencana, 2019.

Jurnal

- Ajiputera, Muhammad Taufik, and Heru Susetyo. 2024. “Implementasi Pengaturan Hak untuk Dilupakan melalui Sistem Penghapusan Data Pribadi dan/atau

- Dokumen Elektronik Menurut Perspektif Hukum Positif di Indonesia.” *Unes Law Review* 6 (3): 8051–67.
- Devara, I Gusti Dama Galang, Anak Agung Sagung Laksmi Dewi, and Ni Made Puspastari Ujianti. 2020. “Perlindungan Hukum Terhadap Data Pribadi Pengguna Jasa Transportasi Online.” *Jurnal Preferensi Hukum* 1 (1): 1–7.
- Fikri, and Rusdiana. 2023. “Ruang Lingkup Perlindungan Data Pribadi: Kajian Hukum Positif Indonesia.” *Ganesha Law Review* 5 (1): 51.
- Parihin, Nela Mardiana. 2023. “Urgensi Perlindungan Data Pribadi dalam Perspektif Hak Asasi Manusia.” *Jurnal Rechten: Riset Hukum dan Hak Asasi Manusia* 5 (1): 16–23. <https://doi.org/10.52005/rechten.v5i1.108>.
- Rayhan, Ahmad, et al. 2024. “Efektivitas Hukum Sistem Pembuktian Alat Bukti Elektronik dalam Ranah Pemeriksaan Bukti di Pengadilan Tata Usaha Negara.” *Jurnal Res Justitia: Jurnal Ilmu Hukum* 4 (1): 279–95.
- Rosadi, Sinta Dewi. 2016. “Konsep Perlindungan Hukum atas Privasi dan Data Pribadi Dikaitkan dengan Penggunaan Cloud Computing di Indonesia.” *Yustisia Jurnal Hukum* 5 (1): 23.
- Setiawan, Ahmad Budi. 2018. “Revolusi Bisnis Berbasis Platform sebagai Penggerak Ekonomi Digital di Indonesia.” *Masyarakat Telematika dan Informasi: Jurnal Penelitian Teknologi Informasi dan Komunikasi* 9 (1): 56–75. <https://doi.org/10.17933/mti.v9i1.118>.
- Solove, Daniel J. 2017. “A Brief History of Information Privacy Law.” *George Washington University Law School Public Law Research Paper* No. 215.
- Tejomurti, Kukuh. 2017. “The Personal Electronic Data Security on the Implementation of Solo Smart City According to the Perspective of Privacy Protection Law.” *Journal of Law, Policy, and Globalization* 66: 1.
- Yolanda, Erlyns, and Rugun Romaida Hutabarat. 2023. “Urgensi Lembaga Pelindungan Data Pribadi di Indonesia Berdasarkan Asas Hukum Responsif.” *Syntax Literate: Jurnal Ilmiah Indonesia* 8 (6): 4175.
- Yunas, Hesty Ananta, and Muhammad Irwan Padli Nasution. 2023. “Perlindungan Hukum Terhadap Privasi Data Pribadi Konsumen Pengguna Gojek di Indonesia.” *Sammajiva: Jurnal Penelitian Bisnis dan Manajemen* 1.3: 69-73.

PERLINDUNGAN DATA PRIBADI DALAM TRANSAKSI ELEKTRONIK MENURUT HUKUM PERDATA DALAM PENGUNA TRANSPORTASI DARING

Peraturan Perundang-Undangan

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945

Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan
Transaksi Elektronik

Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang
Perlindungan Data Pribadi Dalam Sistem Elektronik

Deklarasi Umum Hak Asasi Manusia (DUHAM)

Kovenan Internasional tentang Hak-Hak Sipil dan Politik