JURNAL HUKUM SEHASEN
p-ISSN : 2528-5025
e-ISSN : 2746-6485

Personal Data Protection In The Case Of Covid 19 Vaccine Certificate Data Leak In Wonosobo

Perlindungan Data Pribadi Pada Kasus Kebocoran Data Sertifikat Vaksin Covid 19 Di Wonosobo

Ahmad Reza Syahputra [1)]; Pardamean Harahap [2)]
[1,2)] Universitas Esa Unggul Jakarta
Email: [1)] ahmadreza142003@student.esaunggul.ac.id **;[2)]** idpardamean.harahap@esaunggul.ac.id

ARTICLE HISTORY
Received [04 Agustus 2025]
Revised [01 Oktober 2025]
Accepted [06 Oktober 2025]

KEYWORDS
Personal Data Leaks, Covid-19 Vaccines, Legal Protection, The PDP Law.

ABSTRAK
Pandemi COVID-19 telah mempercepat digitalisasi layanan kesehatan di Indonesia, termasuk penggunaan aplikasi PeduliLindungi untuk sertifikat vaksinasi. Namun, proses pencetakan kartu vaksin fisik melalui pihak ketiga non-resmi di Kabupaten Wonosobo sering menyebabkan kebocoran data pribadi, seperti Nomor Induk Kependudukan (NIK) dan informasi kesehatan, yang disalahgunakan untuk kejahatan siber seperti pinjaman online ilegal. Penelitian ini bertujuan menganalisis ketentuan hukum perlindungan data pribadi berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) serta aplikasinya pada kasus kebocoran data sertifikat vaksin COVID-19 di Wonosobo. Metode penelitian menggunakan pendekatan normatif-empiris, dengan kajian regulasi hukum dan data primer dari wawancara dengan aparat penegak hukum di Polres Wonosobo. Hasil menunjukkan bahwa UU PDP menyediakan kerangka preventif dan represif yang komprehensif, termasuk sanksi pidana hingga 6 tahun penjara dan denda hingga Rp6 miliar, didukung oleh Pasal 28G ayat (1) UUD 1945. Namun, implementasi di Wonosobo lemah akibat minimnya literasi digital masyarakat, kurangnya alat bukti, dan prioritas restorative justice atas penegakan represif, menyebabkan ketidakkonsistenan antara jaminan konstitusional dan praktik lapangan.

ABSTRACT
The COVID-19 pandemic has accelerated the digitalization of health services in Indonesia, including the use of the PeduliLindungi application for vaccination certificates. However, the process of printing physical vaccine cards through unofficial third parties in Wonosobo Regency often leads to the leakage of personal data, such as Population Identification Numbers (NIK) and health information, which are misused for cybercrimes such as illegal online loans. This study aims to analyze the legal provisions of personal data protection based on Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) and its application in the case of COVID-19 vaccine certificate data leak in Wonosobo. The research method uses a normative-empirical approach, with a study of legal regulations and primary data from interviews with law enforcement officials at the Wonosobo Police Station. The results show that the PDP Law provides a comprehensive preventive and repressive framework, including criminal sanctions of up to 6 years in prison and fines of up to Rp6 billion, supported by Article 28G paragraph (1) of the 1945 Constitution. However, implementation in Wonosobo is weak due to the lack of digital literacy of the community, lack of evidence, and the priority of restorative justice over repressive enforcement, causing inconsistencies between constitutional guarantees and field practices.

PENDAHULUAN

Pandemi COVID-19 yang melanda dunia sejak awal tahun 2020 telah mengubah berbagai aspek kehidupan masyarakat global, termasuk di Indonesia. Pemerintah Indonesia merespons situasi darurat ini melalui kebijakan vaksinasi nasional yang diatur dalam Peraturan Presiden Nomor 99 Tahun 2020 tentang Pengadaan Vaksin dan Pelaksanaan Vaksinasi dalam Penanggulangan Pandemi COVID-19. Tujuan utama kebijakan tersebut adalah menekan penyebaran virus, menurunkan angka kematian, serta menciptakan kekebalan kelompok (Martien, 2023).

Sebagai bagian dari pelaksanaan vaksinasi, pemerintah memperkenalkan aplikasi digital PeduliLindungi yang berfungsi menyimpan dan menampilkan sertifikat vaksinasi masyarakat. Namun, aplikasi ini dinilai kurang praktis bagi sebagian masyarakat, khususnya di daerah dengan keterbatasan teknologi atau kelompok usia lanjut. Akibatnya, banyak masyarakat memilih mencetak sertifikat vaksin dalam bentuk kartu fisik untuk memudahkan penggunaan dalam administrasi atau mobilitas di ruang publik.

Permasalahan baru muncul dalam proses pencetakan kartu vaksin, yang sering dilakukan melalui penyedia jasa pihak ketiga tanpa regulasi dan pengawasan yang memadai dalam pengelolaan data pribadi. Untuk mencetak kartu tersebut, masyarakat diminta memberikan informasi sensitif seperti nama lengkap, tanggal lahir, nomor induk kependudukan (NIK), alamat, nomor telepon, hingga tautan ke sertifikat vaksin yang bersifat pribadi. Informasi ini sering dikirimkan melalui aplikasi pesan instan tanpa pengamanan data yang layak, atau bahkan dalam bentuk tangkapan layar maupun file terbuka.

Mekanisme tersebut menjadi celah signifikan dalam perlindungan data pribadi. Data yang seharusnya hanya diketahui oleh pemilik dan lembaga resmi pemerintah justru tersebar ke pihak swasta non-resmi yang tidak memiliki tanggung jawab hukum maupun sistem keamanan informasi yang memadai. Ketidakadaan regulasi teknis atau lisensi resmi untuk jasa cetak kartu vaksin membuat aktivitas ini rentan terhadap pencurian data, penyalahgunaan informasi untuk penipuan, hingga peretasan akun pribadi berbasis data yang bocor (Puteri et al., 2022).Berdasarkan penelitian terkait, minimnya literasi digital, ketidaktahuan masyarakat terhadap bahaya berbagi data pribadi, serta tidak maksimalnya penegakan hukum menjadi penyebab utama kebocoran data. Selain itu, absennya standar baku dalam pengelolaan data vaksin oleh pihak ketiga memperburuk situasi. Perlindungan data pribadi merupakan hak konstitusional sebagaimana diatur dalam Pasal 28G ayat (1) Undang-Undang Dasar 1945. Dalam konteks ini, ketidakmampuan negara dalam memastikan keamanan data masyarakat, terutama selama krisis kesehatan, menunjukkan kelemahan sistem pengawasan serta urgensi perbaikan tata kelola informasi di era digital (Tacino & M. Jefri, 2020).

Jika tidak dikelola dengan hati-hati, data pribadi mudah diakses dan disebarkan di era digital saat ini. Tidak semua individu menyadari pentingnya menjaga keamanan data mereka sendiri, sehingga muncul masalah besar. Meskipun demikian, informasi pribadi seperti NIK dan alamat IP dapat dimanfaatkan untuk berbagai kejahatan digital, seperti penipuan atau pemalsuan identitas. Hak atas privasi setiap orang harus dihormati oleh semua pihak, baik pemerintah, swasta, maupun publik. Dengan meningkatnya penggunaan teknologi dalam berbagai aspek kehidupan, perlindungan data pribadi semakin krusial. Diperlukan regulasi yang kuat dan penegakan hukum yang konsisten untuk memastikan semua orang merasa aman atas perlindungan identitas mereka (Martien, 2023).Pada akhirnya, pandemi COVID-19 menunjukkan betapa pentingnya kebijakan publik, sistem kesehatan, serta manajemen data pribadi di era digital. Ketika teknologi digunakan untuk mempermudah layanan masyarakat, perlindungan data menjadi elemen esensial. Untuk mempertahankan kepercayaan publik dan mencegah kerugian yang lebih besar di masa mendatang, pemerintah, masyarakat, dan pelaku usaha harus bekerja sama membangun sistem yang menjamin keamanan data. Dari latar belakang tersebut, permasalahan utama dalam penelitian ini meliputi: pertama, bagaimana ketentuan hukum dalam perlindungan kebocoran data pribadi; dan kedua, bagaimana analisis perlindungan hukum terhadap kebocoran data pribadi kartu vaksin COVID-19 di Wonosobo.

LANDASAN TEORI

Pengertian Data Pribadi

Data pribadi merujuk pada informasi yang melekat pada individu tertentu, baik yang dapat diidentifikasi secara langsung maupun tidak langsung melalui kombinasi dengan data lain. Menurut Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), data pribadi didefinisikan sebagai data mengenai orang perseorangan yang bersifat spesifik atau dapat diidentifikasi, termasuk nama, nomor identitas, alamat, dan informasi kesehatan seperti status vaksinasi (Kurdi & Cahyono, 2024). Dalam konteks pandemi COVID-19, data pribadi mencakup sertifikat vaksin yang berisi Nomor Induk Kependudukan (NIK), tanggal lahir, dan riwayat vaksinasi, yang jika bocor dapat menimbulkan risiko signifikan terhadap privasi individu.

Perlindungan Hukum Data Pribadi di Indonesia

Perlindungan hukum atas data pribadi di Indonesia didasarkan pada kerangka konstitusional dan undang-undang spesifik. Pasal 28G ayat (1) Undang-Undang Dasar 1945 menjamin hak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda (Ngompat & Maran, 2024). UU PDP Tahun 2022 memperkuat hal ini dengan mengatur pemrosesan, pengumpulan, penyimpanan, dan transfer data pribadi, termasuk larangan pemindahan data lintas negara tanpa persetujuan dan kepastian hukum. Selain itu, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) sebagaimana diubah dengan Undang-Undang Nomor 1 Tahun 2024, melindungi data pribadi dalam media elektronik, dengan sanksi pidana bagi pelanggaran seperti kebocoran data. Dalam kasus kebocoran data sertifikat vaksin, regulasi ini menekankan tanggung jawab pengendali data, seperti pemerintah melalui aplikasi PeduliLindungi, untuk mencegah penyalahgunaan oleh pihak ketiga.

Teori Perlindungan Hukum dan Hak atas Privasi

Teori perlindungan hukum menurut Philipus M. Hadjon membagi perlindungan menjadi preventif (pencegahan) dan represif (penyelesaian sengketa). Dalam konteks data pribadi, teori ini menuntut negara untuk menetapkan regulasi preventif guna menghindari kebocoran, serta mekanisme represif seperti tuntutan hukum bagi korban. Selain itu, teori hak atas privasi dari Warren dan Brandeis menganggap privasi sebagai hak dasar untuk tidak diganggu, yang selaras dengan konsep kedaulatan hukum (Rechtssouvereiniteit) di mana hukum menjadi instrumen utama perlindungan. Di Indonesia,

integrasi ini tercermin dalam pengakuan data pribadi sebagai bagian dari hak asasi manusia, di mana pelanggaran dapat dianggap sebagai pelanggaran konstitusional (Makfirah et al., 2024).

Dampak Kebocoran Data Pribadi

Kebocoran data pribadi, khususnya dalam sertifikat vaksin COVID-19, dapat menyebabkan berbagai dampak negatif, termasuk penyalahgunaan untuk kejahatan siber seperti pinjaman online ilegal (pinjol), pemalsuan identitas, dan penipuan. Data seperti NIK dan informasi kesehatan rawan dieksploitasi, yang tidak hanya merugikan individu secara finansial tetapi juga mengancam keamanan nasional. Studi menunjukkan bahwa pencetakan sertifikat vaksin oleh jasa pihak ketiga tanpa pengawasan meningkatkan risiko ini, karena data sering dibagikan melalui saluran tidak aman seperti pesan instan. Dampak jangka panjang mencakup hilangnya kepercayaan publik terhadap sistem kesehatan digital dan potensi pelanggaran hak asasi manusia (Adhe Pramana et al., 2023).

Kasus Kebocoran Data Sertifikat Vaksin COVID-19 di Wonosobo

Di Kabupaten Wonosobo, kasus kebocoran data sertifikat vaksin COVID-19 sering terjadi melalui jasa pencetakan tidak resmi, di mana masyarakat membagikan data pribadi tanpa pengamanan memadai. Penelitian menyoroti bahwa minimnya regulasi bagi pihak ketiga menyebabkan pencurian data, dengan pelanggaran Pasal 65 UU PDP yang melarang penggunaan data tanpa izin. Kasus serupa secara nasional, seperti kebocoran data PeduliLindungi, menunjukkan ancaman serius terhadap privasi jutaan warga, yang memerlukan penegakan hukum lebih ketat untuk mencegah penyalahgunaan (Ngompat & Maran, 2024).

METODE PENELITIAN

Jenis Penelitian

Penelitian ini menggunakan pendekatan yuridis-empiris dengan metode penelitian kualitatif melalui model deskriptif-analitis. Model ini menitikberatkan pada permasalahan faktual yang terjadi selama penelitian. Pendekatan perundang-undangan yang diterapkan meliputi analisis, interpretasi, dan evaluasi terhadap aspek hukum yang relevan dengan topik yang dibahas. Hal ini membutuhkan pemahaman mendalam mengenai norma-norma hukum, termasuk Undang-Undang, peraturan, dan kebijakan yang berkaitan dengan subjek penelitian.

Sumber Data

Dalam penelitian hukum empiris, data primer didapatkan dari hasil penelitian lapangan. Data lapangan tersebut mencakup informasi yang berasal dari responden, informan, dan juga ahli yang berperan sebagai narasumber.Pada penelitian ini, data primer dihasilkan dari hasil wawancara dengan kepala kepolisian resor wonosbo terkait pelaksanaan percetakan kartu vaksin covid 19. Adapun data sekunder dikumpulkan dari buku, jurnal, makalah hukum, serta berbagai artikel lain yang relevan dengan topik penelitian.

Teknik Pengumpulan Data

Dalam proses pengumpulan data, penulis menggunakan metode wawancara sistematis dengan kepala kepolisian resor Wonosobo serta beberapa warga yang juga menjadi korban kebocoran data pribadi. Dengan demikian, penelitian ini tidak hanya mengandalkan satu narasumber, melainkan memperoleh perspektif langsung dari beberapa pihak yang terdampak.Hal ini dilakukan untuk meningkatkan validitas dan kedalaman data yang dikumpulkan, sekaligus memberikan gambaran nyata mengenai dampak kebocoran data pribadi terhadap masyarakat di Kabupaten Wonosobo. Keberadaan narasumber yang langsung mengalami peristiwa tersebut memperkuat nilai empiris penelitian dan memberikan kontribusi lebih komprehensif terhadap analisis yang dilakukan.

Teknik Analisis Data

Dalam teknik analisis data, penulis mengikuti prosedur pengumpulan data, penyortiran data, penyajian data, kemudian penulis fokuskan dengan menarik kesimpulan terkait kondisi-kondisi yang memengaruhi kebocoran data di wonosobo.

HASIL DAN PEMBAHASAN

Bagaimana Ketentuan Hukum Dalam Perlindungan Kebocoran Data Pribadi

Kebocoran data pribadi terjadi ketika informasi sensitif seseorang, seperti nama, alamat, nomor identitas, atau data keuangan, tersebar tanpa izin ke pihak yang tidak berwenang. Dalam konteks Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi kebocoran ini mencakup

pengungkapan, penggunaan, atau pengaksesan data pribadi yang tidak sah baik melalui sistem elektronik maupun nonelektronik (GRC, n.d.). Undang – undang Perlindungan Data Pribadi sendiri mendefinisikan data pribadi sebagai data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung. Secara umum, Kamus Besar Bahasa Indonesia (KBBI) mendefinisikan "bocor" sebagai suatu keadaan di mana sesuatu (informasi, rahasia, dsb.) yang seharusnya tertutup menjadi tersebar atau diketahui oleh pihak yang tidak berhak (Justice, 2012). Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi mengatur sejumlah pasal yang secara spesifik mengatur tentang kebocoran data pribadi dan akibat hukumnya (Lustarini, 2022).

Tabel 1. Pasal-Pasal Utama UU PDP Terkait Kebocoran Data Pribadi

Pasal	Pokok Isi	Penjelasan Singkat
15	Kewajiban perlindungan keamanan data pribadi selama pemrosesan data	Pengendali data wajib mencegah akses tidak sah, pengubahan, pengungkapan, penyalahgunaan, atau perusakan data.
65	Larangan memperoleh, mengungkap, dan menggunakan data pribadi tanpa hak dan izin	Melarang akses atau penyebaran data pribadi milik orang lain secara melawan hukum.
67	Sanksi pidana bagi pelaku perolehan, pengungkapan, atau penggunaan data pribadi tanpa hak	Ancaman pidana hingga 5 tahun penjara dan/atau denda hingga Rp5 miliar untuk perolehan atau penggunaan data tanpa hak.
68	Sanksi bagi pelaku pemalsuan data pribadi	Pidana hingga 6 tahun penjara dan/atau denda hingga Rp6 miliar jika pemalsuan bertujuan menguntungkan diri atau merugikan orang lain.
57	Sanksi administratif bagi pelanggaran pengelolaan data pribadi	Termasuk peringatan, penghentian kegiatan, penghapusan data, dan denda hingga 2% dari pendapatan tahunan perusahaan.

Sanksi atas kebocoran data pribadi dibedakan menjadi administratif dan pidana, sebagaimana diatur dalam UU PDP. Sanksi ini bertujuan untuk memberikan efek jera dan memastikan akuntabilitas pengendali data, termasuk pemerintah dan pihak swasta. Rincian sanksi disajikan dalam Tabel 2.

Tabel 2. Sanksi atas Kebocoran Data Pribadi Menurut UU PDP

Jenis Sanksi	Rincian	Dasar Hukum
Administratif	Peringatan tertulis, penghentian sementara pemrosesan data, penghapusan data, denda hingga 2% pendapatan tahunan.	Pasal 57
Pidana (Individu)	- Perolehan/mengumpulkan data tanpa hak: Pidana hingga 5 tahun/denda hingga Rp5 miliar. - Pengungkapan data tanpa hak: Pidana hingga 4 tahun/denda hingga Rp4 miliar. - Penggunaan data tanpa hak: Pidana hingga 5 tahun/denda hingga Rp5 miliar. - Pemalsuan data: Pidana hingga 6 tahun/denda hingga Rp6 miliar.	Pasal 67 dan 68
Pidana (Korporasi)	Denda hingga 10 kali lipat dari denda maksimal individu, ditambah sanksi tambahan seperti pembekuan usaha, pencabutan izin, atau pembubaran perusahaan.	Pasal 67 dan 68

Perlindungan Hukum terhadap Kebocoran Data Pribadi

UU PDP mengatur perlindungan hukum preventif dan represif (Galang Surya Mahendra, 2024):

1. Preventif: Setiap pengendali/prosesor wajib menjamin keamanan data, memberitahukan pihak yang datanya bocor, dan memiliki mekanisme mitigasi risiko. Korban berhak mendapatkan pemberitahuan serta dapat meminta penghapusan atau pemusnahan data miliknya.
2. Represif: Korban dapat mengajukan gugatan perdata atas ganti rugi ke pengadilan atau laporan pidana ke kepolisian jika terjadi kebocoran atau penyalahgunaan data (Pasal 64).
3. Pasal 4, 5, 15, 65, 66: Mengatur hak subjek data untuk memperoleh perlindungan, transparansi, dan pemulihan apabila data bocor atau disalahgunakan (JDIH, 2024).

Bentuk perlindungan hukum bagi korban meliputi:

1. Hak atas pemberitahuan dan transparansi dari pengendali data
2. Hak untuk menuntut ganti rugi (perdata)

3. Hak untuk menuntut pelaku secara pidana dan administratif
4. Hak untuk meminta penghapusan/pemusnahan data yang bocor (Situmeang, 2021).

Indonesia telah melihat kemajuan dalam perlindungan data pribadi sejak Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Hukum ini mengatur hak dan kewajiban subjek dan pengendali data serta bagaimana data pribadi dikumpulkan, digunakan, dan disimpan. Perlindungan hukum terdiri dari dua pendekatan utama jika data pribadi bocor, seperti yang terjadi pada kartu vaksin COVID-19 di Wonosobo. Perlindungan Hukum Preventif: Bertujuan untuk mencegah data pribadi disalahgunakan. Menurut UU PDP, pihak pengendali data diharuskan untuk dasar hukum untuk pemrosesan data, Mengawasi sistem elektronik, Jika terjadi kebocoran data, subjek data akan diberitahu. Termasuk juga Pasal 28G ayat (1) UUD 1945, yang menjamin hak setiap orang atas perlindungan diri, kehormatan, dan data di bawah kekuasaannya.

Perlindungan Hukum Represif, Berlaku setelah pelanggaran terjadi, seperti ketika informasi vaksin dibocorkan. Ini dapat termasuk; Sanksi administratif seperti teguran tertulis atau penghentian kegiatan sementara Sanksi pidana yang diatur dalam Pasal 67–70 UU PDP dan UU ITE (UU No. 11 Tahun 2008 jo. UU No. 19 Tahun 2016). kompensasi atau pemulihan bagi individu yang mengalami kerugian akibat kebocoran data. Dengan UU PDP, ketentuan hukum yang kuat untuk mencegah kebocoran data pribadi sudah ada, tetapi masalahnya terletak pada penerapan, pengawasan, dan kesadaran pihak pengendali data, baik pemerintah maupun swasta. Kasus Wonosobo menunjukkan bahwa pelanggaran hak privasi warga dapat terjadi karena penerapan aturan yang tidak disiplin.

Hak konstitusional adalah hak yang dijamin oleh Undang-Undang, hak tersebut dimiliki oleh setiap warga negara sejak mereka lahir hingga meninggal dunia. Hak konstitusional harus dipenuhi oleh negara melalui perlindungan warga negaranya, hal tersebut tertuang dalam kewajiban konstitusional pada pembukaan Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 UUD RI 1945 Alinea Ke-4 yang menyatakan bahwa Negara wajib melindungi segenap bangsa Indonesia dalam meningkatkan kesejahteraan umum, mencerdaskan kehidupan bangsa, dan melaksanakan ketertiban dunia berdasarkan kemerdekaan, perdamaian dunia, serta keadilan sosial Hak konstitusional yang dijelaskan dalam UUD RI 1945. Hak konstitusional warga negara Indonesia berjumlah sekitar 40 dan terjamin dalam Undang-Undang Dasar 1945, mencakup hak-hak mendasar yang mesti dilindungi oleh negara sejak lahir hingga meninggal dunia. Beberapa contoh hak yang sangat berkaitan terutama dengan isu kebocoran data pribadi antara lain: hak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda (Pasal 28G ayat (1)), hak atas rasa aman, hak atas privasi dan kerahasiaan komunikasi (Pasal 28F), hak atas pengakuan dan kepastian hukum yang adil (Pasal 28D ayat (1)), serta hak atas kebebasan berpendapat dan berekspresi (Pasal 28E ayat (3)). Sebagai contoh, hak atas perlindungan diri pribadi mengamanatkan bahwa negara wajib memastikan data pribadi warga terlindungi dari segala bentuk penyalahgunaan atau akses tidak sah.

Perbedaannya dengan kasus kebocoran data pribadi terletak pada realisasi dan perlindungan hak-hak tersebut. Dalam praktiknya, kebocoran data pribadi, seperti pada kasus sertifikat vaksin, menunjukkan kegagalan negara atau pihak yang berkewajiban dalam memenuhi hak atas perlindungan pribadi serta rasa aman warga negara. Contohnya, jika data pribadi yang seharusnya rahasia justru bocor dan disalahgunakan, maka negara telah lalai menegakkan jaminan konstitusional warga atas keamanan, privasi, serta perlindungan dari potensi kerugian. Dengan demikian, setiap kali terjadi kebocoran data pribadi, hal ini pada hakikatnya merupakan pelanggaran terhadap hak konstitusional utama warga yang mestinya menjadi prioritas perlindungan oleh negara dan seluruh pemangku kepentingan.(Utami et al., 2024).

Hak ini menyatakan bahwa warga negara memiliki hak atas perlindungan terhadap diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang berada di bawah kekuasaannya. Meskipun pasal tersebut mengasumsikan bahwa hak pribadi bersifat kepemilikan, berkembangnya teknologi informasi dan komunikasi menuntut agar hak pribadi tidak hanya diartikan sebagai kepemilikan. Hak pribadi seharusnya juga diartikan sebagai hak privasi yang lebih sensitif dan mewakili hak-hak pribadi tersebut. Hak pribadi melibatkan informasi sensitif seperti data pribadi dan identitas seseorang, seperti KTP, SIM, Paspor, KK, NPWP, Nomor Rekening, sidik jari, ciri khas, dan lainnya. Memberikan perlindungan terhadap hak privasi juga berarti memberikan perlindungan terhadap hak kebebasan berbicara. Adanya hak privasi yang melekat pada seseorang memberikan kebebasan untuk dirinya melakukan sesuatu atau tidak melakukan sesuatu terhadap data pribadi nya yang merupakan bagian dari hak asasi yang ia miliki.(PERATURAN PRESIDEN REPUBLIK INDONESIA, 2020)

Indonesia kini telah memasuki era Revolusi Industri 4.0. Semua aspek dapat diatur dari lokasi manapun melalui jaringan internet dan perangkat gawai yang terkoneksi. Dampak dari periode ini sangat signifikan ketika teknologi digital digunakan oleh masyarakat dalam aktivitas sehari-hari, seperti meningkatkan efisiensi kerja, membangun hubungan sosio-ekonomi, dan memberikan kemudahan dalam

berbagai kegiatan. Perkembangan teknologi dan informasi yang berbasis computer berkembang pesat di seluruh kalangan Masyarakat sehingga dengan teknologi tersebut Masyarakat dimudahkan untuk mencari informasi. Peraturan perundang-undangan yang mengatur tentang perlindungan data pribadi yakni Undang-Undang Nomor 8 Tahun 1999 tetang Perlindungan Konsumen, Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik dan Undang-Undang Nomor 7 Tahun Ketentuan-Ketentuan Pokok Kearsipan yang menyatakan bahwa perlindungan konsumen merupakan segala bentuk upaya perlindungan yang menjamin adanya kepastian hukum untuk memberikan perlindungan terhadap konsumen.

Contoh dari perlindungan hukum preventif melibatkan penyusunan peraturan atau undang-undang yang bersifat proaktif untuk mengatur suatu bidang tertentu dengan tujuan mencegah terjadinya praktek-praktek ilegal atau merugikan. Selain itu, kampanye penyuluhan hukum kepada masyarakat juga merupakan bagian dari pendekatan preventif dengan memberikan pemahaman mengenai hak dan kewajiban mereka untuk mencegah pelanggaran hukum. Perlindungan Hukum Preventif bertujuan untuk menciptakan lingkungan hukum yang lebih aman dan menghindari potensi konflik atau pelanggaran sebelum mereka terjadi. Pendekatan ini mencerminkan upaya untuk meminimalkan risiko dan dampak negatif melalui tindakan hukum yang diambil sebelum situasi tersebut mencapai tingkat eskalasi yang serius. Perlindungan hukum ini dituangkan kedalam bentuk pemberian hak dan kewajiban masing-masing pihak yaitu konsumen dan pelaku usaha yang telah diatur di dalam Pasal 4 hingga Pasal 7 Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen.

Perlindungan Hukum Represif, dimana bentuk perlindungan hukum yang ditujukan dalam penyelesaian sebuah sengketa. Penanganan perlindungan hukum bagi masyarakat oleh Pengadilan Umum dan Pengadilan Administrasi merupakan bentuk dari perlindungan hukum represif. Prinsip dari perlindungan hukum bertumpu dan bersumber dari pengertian tentang pengakuan dan perlindungan terhadap hak asasi manusia karena, dari kemunculan konsep pengakuan dan perlindungan terhadap hak asasi manusia ditujukan kepada pembatasan dan peletakan kewajiban masyarakat dan pemerintah.

Tabel 3. Kerangka Hukum Nasional dan Internasional Terkait Perlindungan Data Pribadi

UUD 1945 Pasal 28G (1)	Menjamin hak atas perlindungan diri pribadi dan data pribadi
UU No. 27 Tahun 2022 (UU PDP)	Merupakan regulasi utama perlindungan data pribadi di Indonesia, termasuk hak subjek data, kewajiban pengendali, dan sanksi jika terjadi pelanggaran
UU No. 11 Tahun 2008 jo. UU No. 19 Tahun 2016 (UU ITE)	Mengatur tentang informasi elektronik, termasuk sanksi atas penyalahgunaan informasi pribadi secara ilegal
Perpres No. 39 Tahun 2019 tentang Satu Data Indonesia	Menekankan tata kelola data pemerintah, termasuk data pribadi dalam sistem pemerintahan
Permenkes No. 18 Tahun 2021	Mengatur pelaksanaan vaksinasi nasional, termasuk sistem pencatatan dan penggunaan data kesehatan masyarakat
Universal Declaration of Human Rights (UDHR), Pasal 12	Mengakui hak internasional atas privasi dan larangan intervensi sewenang-wenang terhadap data pribadi

Bagaimana Analisis Perlindungan Hukum Terhadap Kebocoran Data Pribadi Kartu Vaksin Covid 19 Di Wonosobo

Berdasarkan wawancara penulis dengan Kepala Unit Reserse Kriminal Polisi Resor Wonosobo diketahui bahwa memang banyak terjadi pencurian data pribadi, di mana data-data masyarakat di Kota Wonosobo disalah gunakan dengan menginput data- data tersebut untuk pinjaman online. Dalam pinjol ilegal jaminan hanya data pribadi milik korban berupa ktp dan foto dirinya. Jika tidak membayar utang maka akan ditagih menggunakan cacian ataupun ancaman. Jika hal tersebut terjadi maka data korban akan digunakan pemilik aplikasi pinjaman online tersebut untuk digunakan transaksi pinjaman online ilegal di aplikasi lain dengan atas nama korban.

Korban akan ditagih utangnya di aplikasi lain padahal korban tidak merasa mengajukan utang ke aplikasi tersebut dan pasti hutangnya akan lebih banyak. Kepala Unit Reserse Kriminal Polisi Resor Wonosobo menyarankan korban disarankan melapor ke OJK atau ke kantor polisi. Kepala Unit Reserse Kriminal Polisi Resor Wonosobo juga mengatakan bahwa penanganan kasus pencurian data pribadi yang menyebabkan terjadinya penghinaan perorangan mengedepankan kekeluargaan/restorative justice dengan melakukan mediasi yang umumnya dilakukan dengan mengedepankan pendekatan kekeluargaan melalui mediasi yang dilaksanakan minimal dua kali tanpa penahanan, bekerja sama dengan polda dan tim cyber Mabes Polri. Apabila upaya mediasi tersebut tetap tidak menghasilkan

penyelesaian, maka kasus akan dilimpahkan ke kejaksaan, namun pelimpahan ini hanya dapat dilakukan setelah proses mediasi dilakukan setidaknya dua kali. Jika dalam kedua mediasi tidak tercapai kesepakatan atau penyelesaian antar pihak, barulah penanganan perkara berlanjut ke tahap penuntutan formal di kejaksaan untuk diproses sesuai ketentuan perundang-undangan yang berlaku

Kemudian berdasarkan hasil wawancara dengan Kepala Kepolisian Resor Wonosobo AKBP Eko Novan Prasetyopuspito, S.I.K., M.Si yang menyatakan bahwa memang terdapat keluhan di masyarakat mengenai kebocoran data pribadi pada sertifikat vaksin Covid-19, data-data tersebut marak digunakan untuk pengajuan pinjaman *online* namun masyarakat tidak dapat melaporkan kasus-kasus tersebut karena kurangnya alat bukti. Selain itu, AKBP Eko juga menyatakan bahwa kurangnya pengetahuan masyarakat mengenai bahayanya melakukan pencetakan kartu vaksin Covid-19 dan minimnya pengetahuan mengenai regulasi hukum yang mengatur tentang perlindungan data pribadi.

Hingga saat ini, Polres Wonosobo memang menerima beberapa pengaduan masyarakat terkait dugaan kebocoran data vaksin COVID-19 yang pada umumnya terjadi saat pencetakan kartu vaksin di pihak ketiga non-resmi. Namun, seluruh laporan tersebut belum ada yang dapat dilengkapi alat bukti memadai sehingga tidak sampai tahap penetapan tersangka, pemberkasan P21, maupun ke persidangan. Mayoritas diselesaikan secara mediasi dengan langkah edukasi dan peringatan, tanpa proses hukum lebih lanjut. Kasus ini menunjukan perlunya edukasi dan pembenahan sistem pelaporan serta penegakan hukum atas kebocoran data pribadi di tingkat daerah.

Untuk wawancara kedua Bersama bapak Anang dari Kepala Unit Resor Kriminal Polisi Resor Wonosobo terkait dengan faktor penghambat proses pelaporan penyalahgunaan data pribadi adalah dalam penanganan kasus kebocoran data pribadi di tingkat Kepolisian Resor, terdapat kendala utama berupa keterbatasan alat dan sumber daya dalam melacak pelaku tindak pidana digital. Merujuk pada Peraturan Kepolisian Negara Republik Indonesia (Perpol) Nomor 6 Tahun 2019 tentang Penyidikan Tindak Pidana mengatur bahwa apabila ada hambatan dalam proses penyidikan atau keterbatasan kemampuan, Polsek ataupun Polres wajib melakukan koordinasi dan/atau melimpahkan perkara ke tingkat Kepolisian Daerah (Polda) atau Markas Besar Kepolisian (Mabes Polri), guna memastikan kelanjutan proses hukum tidak terhambat. Prinsip kerja "satu atap" di lingkungan Polri mengharuskan sinergi antar unit pada semua tingkatan agar setiap kasus, termasuk pelanggaran privasi data pribadi, tetap dapat dilacak dan ditangani secara optimal meskipun fasilitas atau SDM di tingkat daerah terbatas.

Sejalan dengan tata cara pembuktian pidana, sesuai Ketentuan Pasal 184 Kitab Undang-Undang Hukum Acara Pidana (KUHAP), alat bukti sah dalam perkara pidana harus memenuhi minimal dua alat bukti, yaitu keterangan saksi, keterangan ahli, surat, petunjuk, atau keterangan terdakwa. Praktiknya pada kasus kebocoran data pribadi, alat bukti sering terbatas pada bukti digital seperti percakapan, transfer dana, atau tangkapan layar. Jika hanya dua alat bukti yang sah—misalnya surat elektronik dan rekaman percakapan—sudah terpenuhi sesuai Pasal 184 KUHAP, maka secara normatif polisi dapat melanjutkan proses ke tahap berikutnya. Namun, apabila bukti digital tidak cukup kuat dan sulit diverifikasi validitasnya, maka aparat penegak hukum harus lebih hati-hati dalam melangkah, serta memerlukan koordinasi lebih lanjut atau pelibatan ahli forensik digital agar terpenuhinya unsur pembuktian yang diatur undang-undang, demi menjamin keadilan bagi semua pihak.

Oleh karena itu, perlindungan data pribadi merupakan aspek kewajiban konstitusional yang harus diatur dengan undang-undang. Hingga sekarang, Indonesia masih belum memiliki Undang-Undang atau peraturan yang mengatur tentang Perlindungan Data Pribadi berupa undang-undang khusus. Pengaturan mengenai perlindungan data pribadi masih dalam bentung rancangan undangundang yang masih terus dibahas dan belum disahkan. Padahal dengan banyaknya sengketa yang terjadi yang berkaitan dengan data pribadi, dengan disahkannya Rancangan Undang-Undang Perlindungan Data Pribadi bisa meminimalisir terjadinya kebocoran dan penyalahgunaan data pribadi konsumen dan konsumen merasa aman ketika ingin melakukan kegiatan bisnis maupun transaksi pada e-commerce yang didalamnya wajib memasukkan data pribadi konsumen untuk dapat memenuhi kepentingan konsumen. (Martien, 2023)

Berbeda dengan penghinaan dengan kelompok, agama, dan suku tertentu/SARA penyidik bisa langsung melakukan penyidikan tanpa harus mediasi. Jika tidak menimbulkan kerugian maka polisi tidak dapat melakukan penyidikan. Berdasarkan hasil wawancara tersebut diatas diketahui bahwa kasus-kasus pencurian data pribadi dapat dipertanggungjawabkan apabila menimbulkan kerugian secara materil maupun immaterial bagi pemilik data.

Menurut Satjipto Rahardjo, perlindungan hukum adalah pengayoman terhadap hak asasi manusia yang dirugikan oleh orang lain. Perlindungan hukum diberikan kepada masyarakat agar dapat menikmati semua hak yang diberikan oleh hukum. Namun, C.S.T. Kansil perlindungan hukum adalah berbagai upaya hukum yang harus dilakukan oleh aparat penegak hukum untuk memberikan rasa aman secara pikiran dan fisik dari gangguan dan berbagai ancaman dari pihak mana pun. Philip M. Hadjon mengatakan perlindungan hukum adalah tindakan untuk melindungi atau membantu subjek hukum dengan menggunakan instrumen hukum. Di Indonesia, undang-undang yang mengatur perlindungan

data pribadi konsumen terdiri dari berbagai peraturan yang berbeda dan mengatur perlindungan data pribadi secara umum.(Anggara & Sahya, 2018)

Dalam lima tahun terakhir, masalah data pribadi meningkat. Ini disebabkan oleh pelanggaran teknologi yang membuat semua aktivitas manusia dilakukan secara digital. Kebocoran data sering terjadi karena kemampuan besar teknologi informasi dan komunikasi untuk mengumpulkan, memproses, menyimpan, dan membagikan data. Sangat erat terkait antara keamanan platform dan kebocoran data pribadi karena sistem keamanan platform dapat dibobol dengan mudah.(Edrisy, 2019). Berdasarkan hasil wawancara tersebut diatas diketahui bahwa kasus-kasus pencurian data pribadi dapat dipertanggungjawabkan apabila menimbulkan kerugian secara materil maupun immaterial bagi pemilik data. Terdapat beberapa peraturan perundang-undangan yang mengatur privasi yang dapat digunakan untuk mengakomodir kasus-kasus pencurian data pribadi, yakni: Penyelenggaraan telekomunikasi memiliki kaitan erat dengan transmisi, interkoneksi, dan transfer data dan informasi yang bersifat cepat. Berpindahnya sebuah informasi dan data pribadi dapat terjadi dengan mudah dan cepat. Maka dari itu, untuk menjaga pergerakan informasi dari penyedia telekomunikasi, dalam Pasal 18 ayat (1) mengatur kewajiban penyelenggara telekomunikasi untuk merekam dan menjacatat pemakai jasa telekomunikasi. Kontroversi dalam penegakan hukum dirangkum dalam Tabel 3 berikut, dengan keterkaitan teoritis.

Kontroversi	Persoalan	Keterkaitan Teoritis
Ketidakkonsistenan antara jaminan konstitusional dan praktik	Pasal 28G ayat (1) UUD 1945 menjamin perlindungan data, namun kebocoran tetap marak di Wonosobo.	Teori Hak Asasi Manusia: Privasi adalah hak dasar yang tidak boleh dilanggar.
Prioritas restorative justice	Penanganan lebih mengedepankan mediasi daripada proses hukum formal, mengesankan kejahatan digital tidak serius.	Teori Hadjon: Tindakan represif seperti sanksi harus ditegakkan, bukan hanya mediasi.
Penegakan tidak konsisten	Kasus hanya diproses jika ada kerugian langsung, meskipun pelanggaran privasi sudah cukup.	Teori Hak Asasi Manusia: Pelanggaran tidak mensyaratkan kerugian materiil (Pasal 12 UDHR).
Sistem pencegahan lemah	Minim autentikasi dan audit data di jasa cetak.	Teori Hadjon: Preventif memerlukan regulasi untuk mencegah pelanggaran.
Regulasi tumpang tindih	UU PDP, UU ITE, dan lainnya belum terintegrasi.	Asas lex specialis: UU PDP sebagai acuan utama.
Tidak semua kasus diproses	Hanya jika ada kerugian nyata, menciptakan celah.	Pasal 12 UDHR: Pelanggaran privasi cukup sebagai dasar hukum.

Dampak kebocoran mencakup penyalahgunaan untuk kejahatan siber, hilangnya kepercayaan publik, dan pelanggaran hak konstitusional. Tanggung jawab tidak hanya pada pelaku langsung, tetapi juga pengendali data seperti Kemenkes atau pihak swasta, sebagaimana ditegaskan oleh prinsip akuntabilitas dalam UU PDP. Implementasi regulasi yang lebih ketat, edukasi masyarakat, dan penguatan pengawasan diperlukan untuk mencegah kasus serupa di masa depan.

KESIMPULAN DAN SARAN

Penelitian ini menganalisis perlindungan data pribadi dalam konteks kebocoran data sertifikat vaksin COVID-19 di Wonosobo, dengan fokus pada ketentuan hukum dan aplikasinya. Berdasarkan kajian normatif dan empiris, dapat disimpulkan bahwa Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) menyediakan kerangka hukum komprehensif yang mencakup definisi data pribadi, kewajiban pengendali data, serta sanksi administratif dan pidana untuk mencegah dan menangani kebocoran. Regulasi pendukung seperti Pasal 28G ayat (1) UUD 1945, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), serta instrumen internasional seperti Pasal 12 Universal Declaration of Human Rights (UDHR), menegaskan hak konstitusional atas privasi dan perlindungan data sebagai hak asasi manusia.

Namun, analisis terhadap kasus di Wonosobo menunjukkan bahwa implementasi perlindungan hukum masih lemah. Kebocoran data sering terjadi melalui jasa pencetakan pihak ketiga non-resmi, di mana informasi sensitif seperti Nomor Induk Kependudukan (NIK) dan data vaksinasi dibagikan tanpa pengamanan memadai, menyebabkan penyalahgunaan untuk kejahatan siber seperti pinjaman online ilegal. Penanganan kasus oleh aparat penegak hukum, seperti Polres Wonosobo, cenderung

mengutamakan restorative justice melalui mediasi, dengan kendala utama berupa kurangnya alat bukti dan sumber daya untuk pelacakan digital. Hal ini menimbulkan ketidakkonsistenan antara jaminan konstitusional dan praktik lapangan, di mana pendekatan preventif dan represif belum optimal, sehingga hak atas rasa aman dan privasi masyarakat sering terganggu. Secara keseluruhan, pandemi COVID-19 telah mempercepat digitalisasi layanan kesehatan, tetapi juga mengekspos celah dalam tata kelola data pribadi. Kelemahan literasi digital masyarakat, regulasi yang tumpang tindih, dan prioritas mediasi atas sanksi formal berkontribusi pada berulangnya kebocoran data, yang tidak hanya merugikan individu secara materiil dan immateriil, tetapi juga mengancam kepercayaan publik terhadap sistem pemerintahan digital.

Saran

1. Pemerintah daerah, melalui Dinas Kesehatan dan Komunikasi Informatika, harus menyelenggarakan program penyuluhan rutin kepada masyarakat tentang risiko berbagi data pribadi dan pentingnya menggunakan saluran aman untuk pencetakan sertifikat vaksin. Kolaborasi dengan lembaga pendidikan dapat memperluas jangkauan, terutama bagi kelompok rentan seperti usia lanjut.
2. Kementerian Kesehatan dan Kominfo perlu menetapkan standar lisensi resmi bagi jasa pencetakan sertifikat vaksin, termasuk audit keamanan data secara berkala. Integrasi UU PDP dengan regulasi terkait seperti Perpres Nomor 39 Tahun 2019 tentang Satu Data Indonesia dapat menciptakan sistem terpadu untuk pengelolaan data vaksinasi.
3. Aparat penegak hukum, seperti Polres Wonosobo, disarankan untuk meningkatkan kapasitas sumber daya manusia dan teknologi dalam pelacakan kejahatan siber, dengan mengurangi ketergantungan pada mediasi semata. Penerapan sanksi pidana secara tegas bagi pelaku kebocoran, sesuai Pasal 67 dan 68 UU PDP, akan memberikan efek jera dan memastikan akuntabilitas pengendali data.
4. Diperlukan sinergi antara pemerintah pusat, daerah, swasta, dan masyarakat sipil untuk membangun platform digital yang aman, seperti peningkatan fitur keamanan pada aplikasi PeduliLindungi. Selain itu, pembentukan lembaga pengawas independen untuk data pribadi dapat memantau implementasi regulasi secara berkelanjutan.
5. Penelitian mendatang dianjurkan untuk mengeksplorasi dampak jangka panjang kebocoran data terhadap keamanan nasional dan mengembangkan model perlindungan berbasis teknologi, seperti enkripsi data berbasis blockchain, untuk mencegah kasus serupa di masa depan.

DAFTAR PUSTAKA

Adhe Pramana, A., Irwan Hamzani, A., Taufik, M., & Kata Kunci, A. (2023). Tinjauan Hukum Terhadap Perlindungan Data Pribadi Di Indonesia Bagi Pengguna Vaksin Article.

Anggara, & Sahya. (2018). 5. Buku Hukum Administrasi Negara_merged.

Edrisy, I. fikma. (2019). PENGANTAR HUKUM SIBER.

Galang Surya Mahendra. (2024). Perlindungan Hukum Terhadap Korban Yang Data Pribadi Passportnya Tersebar Akibat Kelalaian Pemerintah. Terang : Jurnal Kajian Ilmu Sosial, Politik Dan Hukum, 1(3), 104–111. https://doi.org/10.62383/terang.v1i3.382

GRC, P. I. (n.d.). 5 Langkah Efektif Atasi Kebocoran Data Pribadi dan Patuhi UU PDP. Proxsis IT GRC. https://it.proxsisgroup.com/5-langkah-efektif-atasi-kebocoran-data-pribadi-dan-patuhi-uu-pdp/

JDIH, A. (2024). Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (PDP): Menjaga Keamanan dan Privasi Data Warga Negara. JDIH Kota Semarang. https://jdih.semarangkota.go.id/artikel/view/undang-undang-nomor-27-tahun-2022-tentang-pelindungan-data-pribadi-pdp-menjaga-keamanan-dan-privasi-data-warga-negara

Justice, M. of. (2012). Personal Data Protection Act. Privacy, 4(1), 1–5.

Kurdi, K., & Cahyono, J. (2024). Perlindungan Data Pribadi di Era Digital Berdasarkan Undang-Undang Nomor 27 Tahun 2022. JUNCTO, 6(2), 330–339. https://doi.org/10.31289/juncto.v6i2.5443

Lustarini, M. (2022). Kepastian Hukum Pelindungan Data Pribadi Pasca Pengesahan UU Nomor 27 Tahun 2022 Mediodecci Lustarini. Kominfo, 1–15.

Makfirah, R., Akbar Nasution, F., & Harris Nasution, A. (2024). Perlindungan Data Pribadi Sebagai Bagian dari Hak Konstitusional Warga Negara dalam Sistem Informasi Partai Politik (SIPOL). JIHHP, 4(5). https://doi.org/10.38035/jihhp.v4i5

Martien, H. D. (2023). Data Pribadi. www.mitrailmumakassar.com

Ngompat, Y. L., & Maran, M. G. M. (2024). Legal development and urgency of personal data protection in indonesia. Journal Indonesia Law and Policy Review (JILPR), 5(3), 627–635. https://doi.org/10.56371/jirpl.v5i3.284

PERATURAN PRESIDEN REPUBLIK INDONESIA (2020). www.hukumonline.com/pusatdata

Situmeang, S. M. T. (2021). Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna Dalam Perspektif Hukum Siber. Sasi, 27(1), 38. https://doi.org/10.47268/sasi.v27i1.394

Utami, F., Kurnianingsih, F., & Edison. (2024). IMPLEMENTASI KEBIJAKAN VAKSINASI COVID-19 DI KOTA BATAM DALAM RANGKA PENANGGULANGAN PANDEMI [Universitas Maritim Raja Ali Haji]. In Jurnal Ilmu Administrasi Negara (Vol. 20, Issue 1). https://lib.umrah.ac.id/