Arus Jurnal Sosial dan Humaniora (AJSH)
Website: http://jurnal.ardenjaya.com/index.php/ajsh
Email: jurnal.ajsh@ardenjaya.com

Upaya Perlindungan Hukum dan Tanggung Jawab Kemkomdigi terhadap Korban Kebocoran Data Pribadi di Indonesia

INFO PENULIS

Fendi Darmawan
Universitas Esa Unggul Jakarta
fendi.big87@student.esaunggul.ac.id

Henry Arianto
Universitas Esa Unggul Jakarta
henry.arianto@esaunggul.ac.id

INFO ARTIKEL

ISSN: 2808-1307
Vol. 5, No. 3, Desember
2025https://jurnal.ardenjaya.com/index.php/ajsh

Saran Penulisan Referensi:

Darmawan, F., & Arianto, H. (2025). Upaya Perlindungan Hukum dan Tanggung Jawab Kemkomdigi terhadap Korban Kebocoran Data Pribadi di Indonesia. *Arus Jurnal Sosial dan Humaniora, 5* (3),3678-3688.

Abstrak

Transformasi digital di Indonesia memunculkan paradoks hukum: negara yang berkewajiban melindungi data pribadi justru menjadi sumber kelalaian sistemik. Serangkaian kebocoran yang melibatkan Kementerian Komunikasi dan Digital (Kemkomdigi) menunjukkan lemahnya akuntabilitas yang sering tersembunyi di balik imunitas negara sebagai regulator. Penelitian ini menelaah batas pertanggungjawaban hukum negara dan upaya hukum warga ketika Lembaga pengawas berubah menjadi pelaku kelalaian. Dengan metode yuridis normatif dan rujukan pada Pasal 17 ICCPR, hasil kajian menunjukkan rezim pelindungan data Indonesia masih bersifat reaktif normatif di atas kertas, tetapi lemah dalam penegakan. Imunitas berlaku ketika Kemkomdigi bertindak sebagai pembuat kebijakan, namun gugatan dapat diajukan jika kelalaian terjadi dalam kapasitasnya sebagai pengendali atau operator data berdasarkan Pasal 1365 KUHPerdata. Warga negara dapat menempuh pengaduan administratif, gugatan perdata, pelaporan pidana atas akses ilegal, atau komunikasi internasional bila mekanisme nasional tidak efektif. Temuan ini menegaskan perlunya batas tegas antara kekebalan regulatif dan tanggung jawab operasional agar pelindungan data pribadi benar-benar menjadi kewajiban hukum yang dapat diuji di pengadilan.

Kata kunci: Kelalaian negara, Tanggung jawab hukum data pribadi, Kemkomdi

Abstract

Indonesia's deepening digital governance exposes a paradox: the state, while mandated to protect citizens' data, often becomes the source of systemic failure. Recurrent breaches involving the Ministry of Communication and Digital Affairs (Kemkomdigi) demonstrate structural negligence masked by bureaucratic immunity. This study probes the legal limits of state accountability and explores remedies when regulatory institutions themselves become violators. Through a normative juridical method and reference to Article 17 ICCPR, the analysis reveals that Indonesia's data protection regime remains reactive heavy in regulation yet weak in enforcement. State immunity operates when Kemkomdigi acts as a regulator, shielding policy making from civil liability, however, once it functions as an operator or data controller, negligence triggers potential liability under Article 1365 of the Civil Code. Citizens may pursue administrative sanctions, civil lawsuits, or criminal proceedings for unlawful access, and if domestic mechanisms fail individual communications before international bodies. The findings affirm that legal certainty demands clearer boundaries between regulatory immunity and operational accountability. Data protection must evolve from declarative rhetoric into enforceable human rights duty, compelling the state to answer not only in policy but beforethe law.

Keywords: State negligence, Personal data protection liability, Kemkomdigi

A. Pendahuluan

Perkembangan teknologi digital telah merevolusi cara masyarakat mengelola informasi dan data pribadi, menciptakan keterhubungan yang masif antara individu dan sistem elektronik. Transformasi ini memang meningkatkan efisiensi di sektor pemerintahan, keuangan, kesehatan, dan komunikasi, namun di sisi lain memperluas potensi pelanggaran privasi akibat lemahnya sistem perlindungan data. Fenomena kebocoran data yang terus berulang menandakan adanya kesenjangan antara kemajuan teknologi dan kesiapan hukum nasional dalam menjamin keamanan informasi warga negara. Kondisi tersebut mendorong peneliti untuk mengkaji isu ini secara mendalam, karena kebocoran data pribadi tidak hanya berdampak pada kerugian ekonomi dan sosial, tetapi juga menjadi ujian serius terhadap tanggung jawab negara dalam menegakkan hak konstitusional atas privasi sebagai bagian dari hak asasi manusia di era digital.

Indonesia sendiri berada dalam kondisi yang mengkhawatirkan karena tingginya kerentanan terhadap pelanggaran privasi digital. Menurut Ogi Prastomiyono, yang menjabat sebagai Kepala Eksekutif Pengawas Industri Asuransi, Penjaminan, dan Dana Pensiun OJK, Indonesia termasuk dalam sepuluh besar negara dengan kasus kebocoran data terbanyak di dunia selama periode 2020 hingga 2024, dengan hampir 100 juta data pribadi yang dilaporkan mengalami kebocoran (CNN Indonesia, 2024). Bahkan juga KEMKOMDIGI melalui siaran pers tertanggal 03 Februari 2025 menyampaikan permohonan maaf atas terjadinya dugaan peretasan yang berdampak pada kebocoran data pegawai, Hal ini diutarakan oleh pejabat Kementerian Komunikasi dan Digital, Alexander Sabar, yang bertanggung jawab sebagai Direktur Jenderal di bidang pengawasan ruang digital (Kementerian Komunikasi dan Digital, 2025). Fenomena kebocoran data yang terus berulang menunjukkan lemahnya sistem pengawasan dan tanggung jawab hukum institusi negara, terutama Kementerian Komunikasi dan Digital (KEMKOMDIGI), yang memiliki mandat konstitusional sebagai pelindung ruang digital nasional.

Hal-hal demikian sangat berdampak buruk bagi para korban kebocoran data, misalnya adalah seperti beresiko dijadikan sebagai korban penipuan, identitas para korban yang bocor sangat rawan dikaitkan dengan suatu tindak kriminal tertentu seperti untuk memesan sejumlah narkoba, senjata, juga identitas tersebut dapat digunakan untuk penipuan dan kejahatan lainnya, data rekam medis yang dilengkapi dengan identitas juga memungkinkan digunakan untuk melakukan kejahatan medis seperti untuk klaim asuransi secara ilegal, lalu di sektor keuangan juga terdapat resiko seperti terjadinya pembobolan rekening, dan yang paling sederhana serta sering dialami adalah banyaknya gangguan dari pihak-pihak yang bertujuan memasarkan ataupun menjual suatu produk tertentu. Artinya dampak dari insiden kebocoran data tersebut tidak hanya bersifat ekonomi, seperti pencurian identitas atau pembobolan rekening, tetapi juga menimbulkan penderitaan psikis bagi korban, termasuk rasa takut,

kecemasan, dan hilangnya rasa aman sebagai warga negara (Suari Anggen Rima Kadek & I Made Sarjana, 2023).

Secara normatif, perlindungan data pribadi di Indonesia berakar pada Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) yang menjadi tonggak utama pengaturan hak subjek data, kewajiban pengendali dan prosesor, serta mekanisme penegakan hukum melalui sanksi administratif, perdata, dan pidana. Regulasi ini menegaskan peran negara dalam menjamin keamanan, keutuhan, dan kerahasiaan data warga negara sekaligus mewajibkan pembentukan lembaga pengawas independen untuk memastikan kepatuhan instansi publik maupun swasta terhadap prinsip transparansi dan akuntabilitas.

Kerangka tersebut diperkuat oleh sejumlah regulasi sektoral yang membentuk ekosistem hukum perlindungan data nasional. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PSTE) mengatur kewajiban penyelenggara sistem elektronik menjaga keamanan berlapis dan menanggung tanggung jawab hukum atas kelalaian teknis. Peraturan Pemerintah Nomor 80 Tahun 2019 tentang Perdagangan Melalui Sistem Elektronik (PMSE) menegaskan perlindungan data konsumen dalam transaksi digital. Di bidang lain, UU ITE, UU Perbankan, UU Telekomunikasi, UU Rumah Sakit, dan UU Administrasi Kependudukan memperkuat prinsip kerahasiaan data pribadi sesuai karakter sektoralnya.Regulasi tersebut menegaskan keseimbangan antara hak publik untuk memperoleh informasi dan hak individu atas perlindungan privasi.

Di atas semua ketentuan sektoral, jaminan konstitusional terhadap privasi berakar pada Pasal 28G ayat (1) UUD 1945, yang melindungi hak setiap orang atas diri pribadi, keluarga, kehormatan, martabat, dan harta benda. Norma ini menempatkan data pribadi sebagai bagian integral dari hak asasi manusia yang tidak dapat dikurangi dalam kondisi apa pun (Rosadi, 2023).

Kerangka hukum nasional menunjukkan upaya integratif dalam membangun sistem perlindungan data pribadi yang komprehensif. Namun, implementasinya masih dihadapkan pada lemahnya koordinasi antar lembaga, ketidaksiapan infrastruktur digital, dan rendahnya akuntabilitas negara saat terjadi kebocoran data di lembaga publik. Kesenjangan antara norma hukum dan praktik tersebut menegaskan pentingnya penegakan prinsip akuntabilitas serta penguatan sistem keamanan siber yang transparan dan berkeadilan. Dalam konteks ini, penelitian berfokus pada dua hal utama: pertama, bagaimana Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi mengatur dan menjamin perlindungan terhadap potensi kebocoran data di Indonesia? dan yang kedua adalah bagaimana bentuk tanggung jawab hukum yang wajib dipenuhi oleh KEMKOMDIGI dalam upaya pencegahan maupun penanganan insiden kebocoran data pribadi yang timbul akibat kelalaian penyelenggara negara?

Untuk menjawab persoalan tersebut, penelitian ini berlandaskan pada Teori Perlindungan Hukum yang dikemukakan oleh *Philipus M. Hadjon*. Teori ini membedakan dua bentuk perlindungan: preventif, yang berfungsi mencegah pelanggaran melalui kebijakan dan regulasi yang efektif, serta represif, yang menitikberatkan pada pemulihan hak korban setelah pelanggaran terjadi. Kerangka ini digunakan untuk menilai sejauh mana peraturan yang berlaku telah memberikan perlindungan pencegahan terhadap kebocoran data pribadi, sekaligus menelaah efektivitas mekanisme penegakan hukum dalam menghadirkan keadilan bagi korban (Hukum Online, 2022).

Pisau analisis kedua yang digunakan adalah Teori Privasi dan Perlindungan Data Pribadi dari *Alan Westin* dan *Lawrence Lessig*. Westin dalam *Privacy and Freedom* memaknai privasi sebagai hak individu untuk mengontrol akses terhadap informasi pribadinya, yang mencakup empat dimensi: *solitude*, *intimacy*, *anonymity*, dan *reserve*. Sementara itu, Lessig melalui teori kode (code theory) menegaskan bahwa perlindungan data tidak hanya bergantung pada hukum tertulis, tetapi juga pada desain dan arsitektur sistem digital yang dapat memperkuat atau justru melemahkan keamanan informasi pribadi (Martien Dhoni, 2023).

Kedua teori tersebut menjadi dasar analisis untuk menilai apakah kegagalan sistem keamanan digital di KEMKOMDIGI merupakan konsekuensi dari lemahnya arsitektur teknologi informasi, kebijakan yang tidak efektif, atau bentuk kelalaian negara dalam memenuhi kewajiban konstitusionalnya sebagaimana diatur dalam Pasal 28G ayat (1) UUD 1945 dan Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia *(UNDANG-UNDANG DASAR NEGARA REPUBLIK INDONESIA 1945, n.d.)* (UNDANG-UNDANG REPUBLIK INDONESIA 39 TAHUN 1999 ASASI MANUSIA, 1999). Integrasi antara Teori Perlindungan Hukum dan Teori Privasi memberikan kerangka berpikir yang menempatkan pelindungan data

pribadi bukan sekadar aspek teknis dalam tata kelola siber, melainkan sebagai manifestasi tanggung jawab hukum negara terhadap hak asasi warganya.

Prinsip state accountability menegaskan bahwa negara, melalui KEMKOMDIGI, wajib mempertanggungjawabkan setiap bentuk kelalaian yang mengakibatkan kebocoran data publik, tanpa dapat berlindung pada dalih serangan digital eksternal. Kegagalan untuk mencegah atau menanggulangi pelanggaran data mencerminkan kelemahan struktural dalam sistem hukum dan tata kelola keamanan nasional. Hal ini diperkuat oleh Peraturan Presiden Nomor 174 Tahun 2024, yang secara eksplisit menetapkan peran KEMKOMDIGI sebagai lembaga sentral dalam pengawasan ruang digital dan pelindungan data pribadi (PERATURAN PRESIDEN REPUBUK INDONESIA 174 TAHUN 2024 KOMUNIKASI DAN DIGITAL, n.d.). Dengan demikian, tanggung jawab hukum negara harus diwujudkan tidak hanya melalui regulasi formal, tetapi juga melalui penegakan prinsip keandalan, transparansi, dan akuntabilitas digital sebagai ukuran nyata perlindungan hak konstitusional warga negara di era teknologi.

Negara diharapkan juga untuk tidak lupa bahwa sebagai bagian dari komunitas global dan anggota *G20*, Indonesia berkewajiban menyesuaikan sistem hukumnya dengan standar internasional agar sejalan dengan praktik terbaik dunia dan menjamin keamanan data lintas batas (*cross-border data flow*). Dalam tataran global, berbagai negara telah lebih dahulu membangun sistem hukum yang komprehensif untuk melindungi data pribadi. Di Eropa, *General Data Protection Regulation (GDPR)* yang berlaku sejak 2018 menjadi standar internasional dengan prinsip-prinsip utama seperti keabsahan, keadilan, transparansi, pembatasan tujuan, dan minimalisasi data (Hummerson, 2024). Ketentuan serupa juga tampak dalam *Malabo Convention* di Afrika (2020) dan *ASEAN Human Rights Declaration* (2012) yang sama-sama menegaskan privasi sebagai bagian dari hak asasi manusia. Ketiga instrumen tersebut mendorong Indonesia untuk menyesuaikan kebijakan hukumnya agar sejalan dengan perkembangan global, terlebih sebagai anggota *G20* yang aktif dalam ekonomi digital lintas batas. Adopsi prinsip-prinsip seperti legitimasi pemrosesan data dan pembatasan tujuan dalam *Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi* menunjukkan bahwa Indonesia berupaya mengharmonisasikan hukum nasional dengan standar internasional, sekaligus menegaskan tanggung jawab negara dalam menjamin hak privasi warganya di ruang digital (Sugiantari Anak Agung Putu Wiwik et al, 2024).

B. Metodologi

Penelitian ini menggunakan metode yuridis normatif yang berfokus pada kajian terhadap prinsip dan ketentuan hukum positif mengenai pelindungan data pribadi. Tujuan utama penelitian ini adalah menganalisis tanggung jawab negara melalui Kementerian Komunikasi dan Digital dalam menangani kebocoran data akibat kelalaian penyelenggara publik. Pendekatan yang digunakan ialah statute approach, melalui penelaahan komprehensif terhadap sejumlah regulasi utama, yaitu Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia, Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, serta Peraturan Presiden Nomor 174 Tahun 2024 tentang Kementerian Komunikasi dan Digital.

Data penelitian bersumber dari bahan hukum primer berupa peraturan perundang-undangan yang bersifat mengikat, serta bahan hukum sekunder seperti literatur akademik dan jurnal hukum terkini yang relevan. Pengumpulan data dilakukan melalui studi kepustakaan (library research), sedangkan analisis dilakukan secara deskriptif kualitatif dengan menafsirkan norma hukum, asas, dan relevansi teorinya terhadap pelindungan data pribadi.

Melalui metode ini, penelitian diharapkan menghasilkan argumentasi hukum yang sistematis, logis, dan kritis dalam menegaskan peran negara sebagai penanggung jawab utama atas pelindungan hak privasi warga negara di era digital.

C. Hasil dan Pembahasan

Sejak diberlakukannya Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP), Indonesia untuk pertama kalinya memiliki kerangka hukum komprehensif yang secara sistematis mengatur pengumpulan, pengelolaan, dan pemrosesan data pribadi. Regulasi ini menegaskan bahwa data pribadi mencakup setiap informasi yang memungkinkan identifikasi seseorang, baik secara langsung maupun melalui penggabungan dengan data lain, dalam sistem elektronik maupun non-elektronik. UU PDP membedakan data pribadi menjadi dua kategori, yaitu data umum dan data spesifik, yang berimplikasi pada tingkat perlindungan

dan standar keamanan yang harus diterapkan oleh pengendali serta prosesor data. Data yang bersifat spesifik, seperti informasi kesehatan, biometrik, atau keuangan, memerlukan mekanisme perlindungan yang lebih ketat dan persetujuan eksplisit dari subjek data sebelum diproses. Secara filosofis, ketentuan dalam UU PDP mencerminkan bahwa pelindungan data pribadi merupakan bagian dari hak asasi manusia sebagaimana dijamin konstitusi, sehingga fungsi pengaturan ini tidak sekadar administratif, tetapi juga konstitusional dalam menjaga kehormatan, martabat, dan privasi individu. Kehadiran UU PDP menandai pergeseran paradigma hukum nasional menuju sistem pelindungan privasi yang lebih progresif, dengan menegaskan tanggung jawab pengendali dan prosesor data, memberikan hak substantif bagi subjek data, menetapkan sanksi atas pelanggaran, serta membentuk lembaga pengawas independen guna memastikan kepatuhan dan akuntabilitas dalam tata kelola data digital di Indonesia (UNDANG-UNDANG REPUBLIK INDONESIA 27 TAHUN 2022 DATA PRIBADI, 2022).

Tingginya frekuensi kebocoran data pribadi di Indonesia tidak dapat dilepaskan dari meningkatnya nilai ekonomis data dalam ekosistem digital modern. Salah satu faktor utama yang memicu maraknya insiden ini adalah tingginya permintaan terhadap data pribadi di pasar, baik untuk kepentingan komersial maupun aktivitas ilegal. Informasi pribadi yang seharusnya bersifat rahasia kini dipandang sebagai komoditas bernilai tinggi yang dapat diperjualbelikan dan dimanfaatkan untuk berbagai kepentingan. Fenomena ini menunjukkan adanya individu, korporasi, maupun kelompok tertentu yang memiliki kepentingan khusus terhadap data pribadi, sehingga mereka aktif mencari, bahkan membeli data tersebut melalui jalur formal maupun informal demi memenuhi kebutuhan atau tujuan spesifik. Di sektor bisnis, data pribadi memiliki nilai strategis karena menjadi fondasi dalam penyusunan kebijakan pemasaran berbasis perilaku konsumen. Melalui data yang diperoleh, pelaku usaha dapat memahami preferensi pelanggan secara detail, menargetkan iklan secara lebih akurat, serta merancang produk dan layanan yang sesuai dengan kebutuhan pasar. Namun, di sisi lain, tingginya permintaan komersial terhadap data ini telah menciptakan pasar gelap data (*dark data market*) yang beroperasi tanpa mekanisme pengawasan yang memadai, sehingga memperluas potensi pelanggaran hak privasi masyarakat (Marshella & Ariawan Gunadi, 2024).

Kondisi diperburuk oleh lemahnya tata kelola keamanan siber dan rendahnya kesadaran perlindungan data di berbagai sektor, banyak institusi publik dan swasta lebih fokus pada aspek administratif, sementara literasi digital rendah, praktik kata sandi tidak aman, dan sistem autentikasi berlapis belum optimal, sehingga celah keamanan dimanfaatkan pihak tidak bertanggung jawab. Selain itu, penegakan hukum yang belum maksimal menciptakan efek impunitas, mempermudah praktik pencurian dan jual-beli data berulang, yang dampaknya menjalar ke kejahatan siber seperti penipuan daring, pemalsuan identitas, pembobolan rekening, klaim asuransi ilegal, hingga penyalahgunaan informasi medis, bahkan penyalahgunaan identitas untuk transaksi terlarang seperti membeli senjata api ilegal dan transaksi narkotika yang menimbulkan beban hukum berat dan tidak semestinya bagi korban kebocoran data pribadi.

Secara struktural, fenomena ini mencerminkan lemahnya sinergi antara kebijakan hukum, kesiapan kelembagaan, dan kapasitas teknis pengelola data, meskipun Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi telah berlaku penuh sejak Oktober 2024, menetapkan hak subjek data, kewajiban pengendali dan prosesor, mekanisme sanksi, serta pembentukan lembaga pengawas independen, implementasi pengawasan dan penegakan hukum masih belum optimal (Gunadi et al, 2023), sehingga terjadi implementation gap antara norma hukum dan realitas sosial yang menghambat terciptanya tata kelola data yang aman, etis, dan menghormati hak asasi manusia (Sutarli & Shelly Kurniawan, 2023).

Kebocoran data pribadi di era digital tidak semata-mata disebabkan oleh ketidakpatuhan individu atau organisasi terhadap regulasi, kelalaian pengguna dalam mengakses layanan digital, atau ketidakhati-hatian pemilik data dalam menyerahkan informasi kepada pihak yang tidak tepat (Gunadi et al, 2023), melainkan merupakan fenomena multi dimensional yang melibatkan faktor teknis, kelembagaan, dan regulatif. Dari sisi teknis, kebocoran dapat terjadi akibat lemahnya standar sistem keamanan yang seharusnya mampu menahan serangan siber, kurang optimalnya prosedur pemulihan bencana (disaster recovery) dan mekanisme pencadangan data, serta ancaman internal berupa oknum dengan akses sah yang menyalahgunakan wewenangnya untuk mencuri atau menyebarkan data dan dapat juga disebabkan oleh kurang kemampuan Sumber Daya Manusia di dalam KEMKOMDIGI itu sendiri seperti yang disampaikan oleh Apryan Anggara Pratama dalam penelitiannya yang berjudul Hacker Bjorka: Pihak Yang Berperan Dalam Mencegah Kebocoran Data, pada bab kesimpulan (Pratama, 2023). Faktor kelembagaan menjadi salah satu penyebab utama tingginya risiko

kebocoran data di Indonesia. Lemahnya fungsi pengawasan pemerintah terhadap penyelenggara sistem elektronik, pengendali, dan pemroses data pribadi membuat praktik pengelolaan data yang tidak aman kerap berlangsung tanpa sanksi yang memadai.

Dari aspek normatif, keberadaan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) memang telah memberikan dasar hukum yang kuat, namun implementasinya masih memerlukan peraturan pelaksana yang lebih teknis agar tanggung jawab pengelola data dapat diatur secara rinci dan operasional. UU PDP melalui Pasal 46 ayat (1) menegaskan bahwa kegagalan dalam pelindungan data mencakup setiap bentuk ketidakmampuan menjaga kerahasiaan, integritas, maupun ketersediaan data, termasuk pengungkapan, kehilangan, perubahan, atau akses tidak sah. Rumusan ini sejalan dengan prinsip General Data Protection Regulation (GDPR) yang menempatkan pelanggaran data sebagai bentuk kegagalan sistemik akibat lemahnya pengendalian, kelalaian teknis, atau akses tanpa otorisasi terhadap informasi pribadi. Namun demikian, efektivitas pengaturan tersebut masih terbatas pada tataran normatif, karena belum sepenuhnya didukung oleh mekanisme pengawasan dan penegakan hukum yang konsisten. Hal ini juga menjadi perhatian dalam penelitian M. Rafifnafia Hertianto yang menyoroti lemahnya sistem penegakan hukum terhadap kegagalan pelindungan data pribadi di Indonesia (Hertianto, 2021).

Sebagai dasar konseptual, teori perlindungan hukum merupakan pilar utama dalam prinsip negara hukum yang menegaskan kewajiban negara untuk melindungi hak-hak warga negara, termasuk hak atas data pribadi di ruang digital. Gagasan ini diperkenalkan oleh Philipus M. Hadjon, yang menekankan bahwa perlindungan hukum berfungsi menjaga martabat dan hak asasi individu melalui dua mekanisme utama, yaitu preventif dan represif. Perlindungan preventif bertujuan mencegah potensi pelanggaran dengan memberikan ruang bagi masyarakat untuk menolak atau mengajukan keberatan atas kebijakan yang berisiko, seperti proses verifikasi dan persetujuan pengelolaan data oleh penyelenggara sistem elektronik. Sementara itu, perlindungan represif berfokus pada penyelesaian pelanggaran yang telah terjadi, antara lain melalui mekanisme pengaduan, penegakan sanksi, atau gugatan perdata terhadap pihak yang lalai menjaga keamanan data. Relevansinya dengan isu kebocoran data pribadi tampak jelas, karena setiap kegagalan sistem keamanan merupakan bentuk pelanggaran hak individu yang memerlukan respon hukum, baik pencegahan maupun pemulihan. Sejalan dengan pemikiran Setiono, perlindungan hukum juga mengandung kewajiban negara untuk mencegah penyalahgunaan kewenangan oleh pengendali maupun pemroses data, serta memastikan setiap aktivitas pengelolaan informasi berjalan sesuai prinsip kehati-hatian, akuntabilitas, dan kepatuhan terhadap norma hukum yang berlaku (Hukum Online, 2022).

Sebagai landasan teori kedua, teori hak privasi dan pelindungan data pribadi berakar dari perkembangan konsepsi klasik *ius*, yang pada mulanya dimaknai sebagai "keadilan" dan kemudian berevolusi menjadi pengakuan terhadap hak-hak individual. Cikal bakal konsep ini mulai tampak dalam *Decretum Gratiani* di Bologna pada abad ke-12, yang menegaskan perlindungan atas kehidupan pribadi sebagai bagian dari martabat manusia. Gagasan hak privasi modern secara tegas dikemukakan oleh Samuel D. Warren II dan Louis D. Brandeis melalui artikel monumental *The Right to Privacy* yang diterbitkan dalam *Harvard Law Review* tahun 1890. Dalam tulisan tersebut, privasi diartikulasikan sebagai hak fundamental untuk bebas dari gangguan dan kontrol atas informasi pribadi, sekaligus sebagai bentuk perlawanan terhadap penyalahgunaan data oleh pihak lain. Pemikiran ini kemudian menjadi fondasi teoretis bagi sistem hukum modern dalam mengatur pelindungan data pribadi di era digital (Furqania & Ahmad Sholikhin Ruslie, 2023).

Teori hak privasi kemudian dikembangkan secara komprehensif oleh Alan Westin dalam karyanya *Privacy and Freedom*(1967), yang memaknai privasi sebagai hak setiap individu, kelompok, atau lembaga untuk mengendalikan akses terhadap informasi pribadinya. Westin menguraikan bahwa privasi memiliki empat dimensi utama, yakni *solitude*se bagai hak untuk menyendiri tanpa gangguan eksternal, *intimacy* sebagai kebebasan membangun hubungan personal tanpa campur tangan pihak lain, *anonymity* sebagai hak untuk tetap tidak teridentifikasi di ruang publik, dan *reserve* sebagai kemampuan individu mengatur sejauh mana informasi pribadinya dapat diakses atau diungkapkan kepada publik. Melalui klasifikasi ini, Westin menegaskan bahwa privasi merupakan bentuk kendali otonom individu atas batas antara ranah publik dan privat, yang menjadi fondasi bagi pengaturan pelindungan data pribadi dalam konteks hukum modern (Aruan Soritua Elkana Jonathan, 2024).

Pemikiran mengenai hak privasi kemudian dikembangkan lebih lanjut oleh Lawrence Lessig melalui karyanya *Code and Other Laws of Cyberspace* (1999), yang menegaskan bahwa perlindungan privasi di era digital tidak dapat hanya bergantung pada instrumen hukum formal.

Menurut Lessig, efektivitas pelindungan data harus dibangun melalui empat pendekatan yang saling melengkapi, yakni regulasi hukum untuk menentukan batas pelanggaran dan sanksi, norma sosial yang berperan membentuk budaya kepatuhan serta kepercayaan publik, mekanisme pasar yang mendorong penyedia layanan digital merancang kebijakan privasi yang bertanggung jawab, serta arsitektur teknologi (code) yang berfungsi sebagai instrumen pengendali agar sistem informasi aman dari penyalahgunaan data. Melalui keempat instrumen ini, Lessig menempatkan kode dan desain sistem digital sejajar dengan hukum sebagai sarana pengaturan perilaku di ruang siber, sehingga keamanan data menjadi hasil sinergi antara regulasi, etika, ekonomi, dan teknologi (Lessig, 1999).

Teori hak privasi memiliki relevansi langsung terhadap persoalan kebocoran data pribadi di Indonesia, karena memberikan dasar konseptual untuk menafsirkan hak individu atas kendali informasi pribadinya serta menguji sejauh mana efektivitas pelaksanaan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Melalui pendekatan ini, privasi dipahami tidak hanya sebagai hak moral, tetapi juga sebagai hak hukum yang menuntut perlindungan konkret melalui mekanisme yang komprehensif, mulai dari penegakan hukum, penerapan standar etika industri, kebijakan perusahaan yang transparan, hingga penguatan arsitektur teknologi yang aman. Dengan demikian, teori ini memperluas pemahaman bahwa pelindungan data pribadi merupakan bagian dari jaminan hak konstitusional warga negara yang wajib dijaga oleh negara dalam setiap aktivitas pemrosesan data di ruang digital.

Pembahasan mengenai Bagaimana Ketentuan Hukum dalam UU PDP Mengatur dan Menjamin Perlindungan terhadap Potensi Kebocoran Data di Indonesia?

Perlindungan data pribadi menjadi isu hukum strategis di Indonesia seiring dengan meningkatnya digitalisasi layanan publik dan aktivitas ekonomi berbasis data. Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) telah menetapkan kerangka normatif yang mencakup hak subjek data, kewajiban pengendali dan prosesor data, serta mekanisme ganti rugi bagi korban kebocoran data sebagaimana diatur dalam Pasal 12 ayat (1). Namun, hingga saat ini belum diterbitkan Peraturan Pemerintah (PP) yang mengatur lebih lanjut tata cara pelaksanaan hak ganti rugi tersebut, termasuk prosedur penilaian kerugian dan mekanisme penyelesaiannya. Ketiadaan aturan pelaksana ini menimbulkan kekosongan hukum (legal vacuum) yang berpotensi melemahkan posisi korban dalam memperoleh keadilan. Kondisi tersebut menunjukkan adanya disparitas antara norma substantif dan efektivitas implementasi, di mana pemerintah, melalui Kementerian Komunikasi dan Digital (KEMKOMDIGI), masih menghadapi tantangan dalam memastikan kepatuhan para penyelenggara sistem elektronik terhadap prinsip-prinsip pelindungan data pribadi.

Selain itu, meskipun sebagian ketentuan Pasal 46 UU PDP yang mengatur tentang kewajiban menjaga kerahasiaan, integritas, dan ketersediaan data telah tercermin dalam Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PSTE), regulasi tersebut masih terbatas pada aspek teknis dan belum mengatur secara rinci mengenai standar audit keamanan data, prosedur notifikasi kebocoran, maupun bentuk sanksi preventif dan represif. Akibatnya, tingkat kepatuhan antarpenyelenggara sistem elektronik masih beragam, sementara penegakan hukum terhadap insiden kebocoran data belum menunjukkan konsistensi (Yudistira & Ramadani, 2023).

Dalam perspektif teori perlindungan hukum, kondisi ini memperlihatkan bahwa negara belum sepenuhnya menjalankan kewajiban konstitusionalnya untuk menjamin hak privasi warga negara melalui instrumen hukum yang jelas dan dapat diterapkan secara efektif. Dengan demikian, penerbitan PP pelaksana UU PDP menjadi mendesak, agar mekanisme ganti rugi dan akuntabilitas negara dalam perlindungan data pribadi dapat berjalan sesuai prinsip keadilan dan kepastian hukum di era digital.

Kelemahan penerapan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) terlihat dari maraknya kebocoran data di sektor publik maupun swasta yang menunjukkan belum efektifnya instrumen hukum dalam menjamin keamanan informasi pribadi. Salah satu persoalan mendasar adalah belum diterbitkannya Peraturan Pemerintah (PP) sebagai aturan pelaksana, terutama yang mengatur mekanisme audit keamanan, standar perlindungan data yang seragam, serta tata cara pemberian ganti rugi bagi korban pelanggaran. Kekosongan hukum ini memperlemah posisi subjek data sekaligus menghambat penegakan prinsip akuntabilitas dalam pengelolaan data. Dalam konteks teori perlindungan hukum, negara memiliki kewajiban konstitusional untuk menjamin hak atas privasi dan keamanan digital warganya melalui regulasi yang jelas, pengawasan yang efektif, serta penegakan hukum yang tegas. Namun, efektivitas UU PDP masih sangat bergantung pada kapasitas Kementerian Komunikasi dan Digital (KEMKOMDIGI) dalam mengimplementasikan langkah teknis dan

kelembagaan yang terukur agar perlindungan data pribadi tidak berhenti sebagai norma deklaratif, melainkan menjadi jaminan hukum yang nyata di ruang digital (Aruan Soritua Elkana Jonathan, 2024).

Pembahasan mengenai Bagaimana bentuk tanggung jawab hukum yang harus dipenuhi oleh Kementerian Komunikasi dan Digital dalam rangka pencegahan dan penanganan kebocoran data pribadi?

Sebelum menilai tanggung jawab hukum Kementerian Komunikasi dan Digital (KEMKOMDIGI) atas kebocoran data pribadi, perlu dipahami bahwa kerugian korban bersifat kompleks, mencakup aspek material dan immaterial. Kerugian material meliputi kehilangan kendali atas identitas dan data finansial, risiko pencurian identitas, serta penyalahgunaan informasi sensitif seperti NPWP dan KTP elektronik. Sementara itu, kerugian immaterial mencakup pelanggaran privasi, rusaknya reputasi, tekanan psikologis, dan hilangnya kendali atas informasi pribadi yang seharusnya dilindungi.

Dalam perspektif Alan Westin, privasi merupakan hak individu untuk menentukan batas akses terhadap data pribadinya, sedangkan Lawrence Lessig melalui *code theory* menekankan bahwa perlindungan tidak hanya dibentuk oleh hukum tertulis, tetapi juga oleh arsitektur digital yang aman. Kebocoran data karenanya tidak sekadar pelanggaran administratif, tetapi pelanggaran terhadap otonomi dan martabat manusia.

Berdasarkan Teori Perlindungan Hukum Philipus M. Hadjon, pendekatan preventif harus diwujudkan melalui regulasi dan kebijakan yang efektif untuk mencegah pelanggaran, sedangkan pendekatan represif berfungsi memulihkan hak korban melalui kompensasi yang adil. Dengan demikian, kebocoran data memiliki implikasi multidimensional: hukum, sosial, dan psikologis yang menguji efektivitas sistem perlindungan negara terhadap hak atas privasi sebagaimana dijamin oleh Pasal 28G ayat (1) UUD 1945 dan UU No. 39 Tahun 1999 tentang Hak Asasi Manusia.

Kementerian Komunikasi dan Digital (KEMKOMDIGI) memikul tanggung jawab hukum strategis untuk mencegah dan menangani kebocoran data pribadi di Indonesia melalui langkah-langkah preventif yang sistematis, sejalan dengan prinsip Teori Perlindungan Hukum Philipus M. Hadjon serta teori hak atas privasi Westin dan Lessig, sekaligus berperan sebagai pemberi usul kepada pemerintah untuk segera menerbitkan seluruh Peraturan Pemerintah (PP) pelaksana UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) yang hingga kini belum tersedia, termasuk PP terkait mekanisme ganti rugi, audit berkala, dan standar perlindungan data. Kekosongan PP pelaksana, ditambah rendahnya literasi digital masyarakat, menjadi faktor utama maraknya insiden kebocoran data di sektor publik maupun swasta, seperti kebocoran data NPWP masyarakat dan data pegawai KEMKOMDIGI. Secara preventif, KEMKOMDIGI wajib menetapkan standar keamanan siber seragam bagi seluruh Penyelenggara Sistem Elektronik (PSE), meningkatkan kompetensi SDM di bidang keamanan informasi, menugaskan pejabat pengelola data profesional, dan menyelenggarakan edukasi publik mengenai hak-hak subjek data serta mitigasi risiko kebocoran. Secara filosofis, hak atas privasi menurut Westin mencakup empat dimensi: solitude, intimacy, anonymity, dan reserve yang menekankan kontrol individu terhadap informasi pribadinya, sementara Lessig menegaskan bahwa perlindungan privasi juga sangat bergantung pada desain dan arsitektur sistem digital (Martien, 2023).

Selain itu, KEMKOMDIGI sebagai lembaga negara memiliki kewajiban konstitusional dan strategis untuk menjaga keamanan ekosistem ruang digital Indonesia, memastikan seluruh mekanisme perlindungan data sesuai Pasal 28G UUD 1945, UU No. 39 Tahun 1999 tentang Hak Asasi Manusia, serta prinsip internasional yang diakui dalam UDHR Pasal 12 dan ICCPR Pasal 17 terkait hak privasi sebagai hak asasi setiap individu. Sementara itu, PP No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PSTE) hanya sebagian mengakomodasi ketentuan Pasal 46 UU PDP, sehingga audit berkala, sanksi preventif, dan standar perlindungan data seragam belum diterapkan secara optimal, menimbulkan kesenjangan antara regulasi substantif dan implementasi teknis. Dengan menjalankan seluruh tanggung jawab preventif, mengusulkan PP pelaksana yang komprehensif, memperkuat pengawasan, melakukan audit berkala, dan menyelenggarakan edukasi publik secara konsisten, KEMKOMDIGI tidak hanya berfungsi sebagai regulator, tetapi juga sebagai penanggung jawab utama keamanan ekosistem digital nasional, sehingga risiko kebocoran data dapat diminimalkan dan hak-hak subjek data terlindungi secara optimal.

Berdasarkan analisis, implikasi yuridis dari kegagalan Kementerian Komunikasi dan Digital (KEMKOMDIGI) dalam melindungi data pribadi adalah terbukanya ruang bagi masyarakat untuk menempuh upaya hukum represif. Namun dengan maksud ingin menambahkan apa yang

sudah diteliti oleh peneliti sebelumnya yaitu Anak Agung Putu Wiwik Sugiantari melalui penelitiannya yang berjudul Analisis Sanksi Hukum Atas Pertanggungjawaban Pemerintah Terhadap Insiden Bocornya Data Pribadi Masyarakat Dari Pusat Data Nasional (PDN) Indonesia pada bab kesimpulan (Sugiantari Anak Agung Putu Wiwik et al, 2024), bahwa menurut pandangan Kami, akuntabilitas hukum KEMKOMDIGI perlu didudukkan secara proporsional dengan membedakan peran gandanya sebagai regulator dan operator. Pertama, ketika KEMKOMDIGI berfungsi sebagai pelaksana (operator) atau pengawas, kelalaiannya dapat menjadi subjek gugatan Perbuatan Melawan Hukum (PMH) berbasis Pasal 1365 KUHPerdata. Gugatan ini relevan ketika terjadi tindakan faktual yang merugikan (*feitelijke handeling*), bukan pada proses pembuatan kebijakan. Sebagai contoh konkret, jika KEMKOMDIGI gagal melaksanakan audit keamanan berkala yang diamanatkan regulasi pada Penyelenggara Sistem Elektronik (PSE) berisiko tinggi, atau lalai dalam menerapkan tambalan keamanan (*security patch*) pada sistem data yang dikelolanya secara langsung, maka omisi tersebut merupakan bentuk kelalaian operasional. Dalam litigasi semacam ini, asas pembuktian terbalik dapat diterapkan: korban hanya perlu membuktikan adanya kerugian, sementara KEMKOMDIGI sebagai tergugat harus mampu menunjukkan bahwa seluruh kewajiban preventif telah dilaksanakan secara patut. Opsi gugatan, baik secara individual maupun melalui mekanisme class action (Harahap, 2017), menjadi semakin relevan mengingat ketiadaan Peraturan Pemerintah (PP) pelaksana UU PDP yang menimbulkan kekosongan hukum terkait prosedur ganti rugi formal.

Sebaliknya, akuntabilitas hukum melalui Pasal 1365 KUHPerdata tidak berlaku ketika KEMKOMDIGI bertindak dalam kapasitasnya sebagai regulator. Tindakan dalam ranah ini, seperti merumuskan atau bahkan terlambat menerbitkan sebuah peraturan, diklasifikasikan sebagai kebijakan publik (*beleidsregel*). Tindakan regulatif ini memiliki imunitas dari tuntutan perdata karena pengujian terhadap materi atau proses pembentukan sebuah kebijakan bukanlah kompetensi pengadilan perdata, melainkan dapat melalui mekanisme pengujian perundang-undangan di Mahkamah Konstitusi jika dianggap ada isi dari Undang-Undang yang berkonflik dengan Undang-Undang Dasar 1945, atau melalui mekanisme yang disediakan oleh Mahkamah Agung jika ada konflik dengan peraturan perundang-undangan lainnya, maupun melalui mekanisme yang difasilitasi Pengadilan Tata Usaha Negara. Sebagai contoh, masyarakat tidak dapat menggugat KEMKOMDIGI atas kerugian yang timbul akibat keterlambatan penerbitan PP pelaksana UU PDP, karena hal tersebut merupakan bagian dari proses politik dan administratif di ranah eksekutif.

Lebih lanjut, apabila jalur litigasi nasional tidak memberikan remediasi yang efektif, kegagalan negara dalam melindungi privasi data pribadi berpotensi diklasifikasikan sebagai pelanggaran hak asasi manusia sebagaimana dijamin dalam Pasal 17 ICCPR. Kondisi ini membuka kemungkinan bagi korban untuk mengakses forum hukum internasional (Buchan & Lubin, n.d.).

D. Kesimpulan

Berdasarkan dua rumusan masalah, penelitian berjudul *"Upaya Perlindungan Hukum dan Tanggung Jawab Negara terhadap Korban Kebocoran Data Pribadi di Indonesia"* menyimpulkan bahwa Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) telah membentuk dasar hukum komprehensif dalam menjamin hak atas keamanan data warga negara melalui pengaturan hak subjek data, kewajiban pengendali dan prosesor data, serta mekanisme kompensasi bagi korban pelanggaran. Namun, efektivitas norma tersebut masih terbatas karena Peraturan Pemerintah pelaksana belum diterbitkan, sehingga prosedur audit keamanan, standar perlindungan data, dan tata cara pemberian ganti rugi belum memiliki landasan operasional yang jelas. Kekosongan ini menimbulkan celah hukum yang dapat melemahkan akuntabilitas negara dan perlindungan privasi publik.

Dalam konteks tanggung jawab hukum, Kementerian Komunikasi dan Digital (KEMKOMDIGI) memegang peran ganda sebagai regulator yang menetapkan kebijakan, dan sebagai pelaksana pengawasan serta pengelola sistem digital. Ketika bertindak sebagai regulator, tindakan atau kelalaian yang timbul karena belum rampungnya kebijakan tidak dapat digugat berdasarkan Pasal 1365 KUHPerdata.

Namun, dalam fungsi operasionalnya, kelalaian yang menyebabkan kebocoran data membuka peluang gugatan perdata dengan penerapan asas pembuktian terbalik, di mana korban cukup membuktikan adanya kerugian, sementara kementerian wajib menunjukkan itikad baik dan kepatuhan terhadap prosedur pengamanan data. Dalam konteks internasional,

kelalaian negara dalam melindungi data pribadi dapat dikategorikan sebagai pelanggaran hak asasi manusia, karena menyentuh hak fundamental atas privasi sebagaimana tercantum dalam *International Covenant on Civil and Political Rights* (ICCPR) Pasal 17.

Selain itu, korban juga dapat menempuh jalur pidana melalui Pasal 332–335 KUHP Baru (UU No. 1 Tahun 2023) jika kebocoran melibatkan penyalahgunaan akses elektronik oleh pejabat berwenang (Redaksi Sinar Grafika, 2023).

Secara keseluruhan, efektivitas pelindungan data pribadi di Indonesia menuntut pembentukan peraturan turunan UU PDP, peningkatan kapasitas kelembagaan KEMKOMDIGI, pengawasan berkelanjutan, serta penegakan hukum yang tegas dan transparan untuk menjamin hak konstitusional warga negara atas privasi digital secara nyata.

E. Referensi

Aruan Soritua Elkana Jonathan. (2024). Perlindungan Data Pribadi Ditinjau Dari Teori Perlindungan Hukum Dan Teori Perlindungan Hak Atas Privasi. In *Jurnal Globalisasi Hukum* (Vol. 1, Issue 1). https://e-journal.trisakti.ac.id/index.php/globalisasihukum/issue/view/1187DOI:https://doi.org/xxxxxx

Buchan, R., & Lubin, A. (n.d.). *The Rights to Privacy and Data Protection in Times of Armed Conflict Autonomous Cyber Capabilities under International Law*.

CNN Indonesia. (2024). *27 November pukul 16.39 WIB,*. "*RI Masuk 10 Besar Negara Kebocoran Data Tertinggi, Hampir 100 Juta Data.*"

Furqania, A. M., & Ahmad Sholikhin Ruslie. (2023). Indonesia Journal of Law and Social-Political Governance, berjudul TANGGUNG GUGAT PEMERINTAH DALAM PERLINDUNGAN DATA PRIBADI, bab pendahuluan. *Bureaucracy Journal: Indonesia Journal of Law and Social-Political Governance*, *3*, 488. https://doi.org/10.53363/bureau.v3i1.195

Gunadi et al. (2023). Proceeding of Conference on Law and Social Studies, berjudul Perlindungan Hukum Atas Kebocoran Data Pribadi. *Universitas Pelita Harapan*. http://prosiding.unipma.ac.id/index.php/COLaS

Harahap, Y. (2017). *Hukum Acara Perdata Tentang Gugatan, Persidangan, Penyitaan, Pembuktian, dan Putusan Pengadilan. Jakarta : Sinar Grafika.188*.

Hertianto, M. R. (2021). Jurnal Hukum, berjudul Sistem Penegakan Hukum Terhadap Kegagalan Dalam Perlindungan Data Pribadi Di Indonesia. *Jurnal Hukum Fakultas Hukum Gajah Mada*, *43*, 96.

Hukum Online. (2022). *Artikel berita media daring HUKUM ONLINE tertanggal 30 September 2022, yang berjudul "Teori-Teori Perlindungan Hukum Menurut Para Ahli."*

Hummerson, A. W. (2024). *Buku Perlindungan dan tanggungjawab hukum kebocoran data pribadi dalam transaksi elektronik : pasca terbitnya UU PDP no. 27 tahun 2022* (pertama). Yogyakarta: Genta Publishing.

Kementerian Komunikasi dan Digital. (2025). *Siaran Pers pada halaman berita website resmi KOMDIGI yang dipublikasikan pada tanggal 3 Februari*. *"Kemkomdigi Investigasi Dugaan Kebocoran Data Pegawai"*.

Lessig, L. (1999). Issue 1 Article 4 1999 Part of the Privacy Law Commons Recommended Citation Recommended Citation Lawrence Lessig, The Architecture of Privacy: Remaking Privacy in Cyberspace. In *Technology Law Vanderbilt Journal of Entertainment & Technology Law* (Vol. 1). https://scholarship.law.vanderbilt.edu/jetlawAvailableat:https://scholarship.law.vanderbilt.edu/jetlaw/vol1/iss1/4

Marshella, C., & Ariawan Gunadi. (2024). *Jurnal Hukum Lex Generalis, Konsep Tanggung Jawab Negara Terhadap Kewajiban Melindungi Data Pribadi Masyarakat di Indonesia (Studi Kasus Kebocoran Data NPWP Masyarakat Indonesia) bab Pendahuluan*.

Martien Dhoni. (2023). *Perlindungan Hukum Data Pribadi. Makasar : Mitra Ilmu. 29-35*. http://repo.jayabaya.ac.id/id/eprint/4449

PERATURAN PRESIDEN REPUBUK INDONESIA NOMOR 174 TAHUN 2024 TENTANG KEMENTERIAN KOMUNIKASI DAN DIGITAL. (n.d.).

Pratama, A. A. (2023). *Jurnal Hukum Magnum Opus, berjudul Hacker Bjorka: Pihak yang Berperan dalam Mencegah Kebocoran Data*. *6*, 22–22.

Redaksi Sinar Grafika. (2023). *Kitab Undang-Undang Hukum Pidana 2023. Jakarta:Sinar Grafika.* 105–106.

Rosadi, S. D. (2023). *Pembahasan UU Perlindungan Data Pribadi (UU RI NO.27 TAHUN 2022), Cetakan pertama, Jakarta: Sinar Grafika, 2023, Print*.

Suari Anggen Rima Kadek, & I Made Sarjana. (2023). "MENJAGA PRIVASI DI ERA DIGITAL: PERLINDUNGAN DATA PRIBADI DI INDONESIA" pada bab pendahuluan, Alinea ke-4. *Jurnal Analisis Hukum*, *6*.

Sugiantari Anak Agung Putu Wiwik et al. (2024). Jurnal Hukum Saraswati, berjudul Analisis Sanksi Hukum Atas Pertanggungjawaban Pemerintah Terhadap Insiden Bocornya Data Pribadi Masyarakat Dari Pusat Data Nasional (PDN) Indonesia, bab kesimpulan. *Jurnal Hukum Saraswati (JHS),Volume. 06, Nomor 02, (2024)*, *06*, 738.

Sutarli, A. F., & Shelly Kurniawan. (2023). Journal Of Social Science Research, berjudul "Peranan Pemerintah Melalui Undang-Undang Perlindungan Data Pribadi dalam Menanggulangi Phising di Indonesia", bab Simpulan. *INNOVATIVE: Journal Of Social Science Research Volume 3 Nomor 2*, *3*.

UNDANG-UNDANG DASAR NEGARA REPUBLIK INDONESIA 1945. (n.d.). *UNDANG-UNDANG DASAR NEGARA REPUBLIK INDONESIA 1945*.

UNDANG-UNDANG REPUBLIK INDONESIA NOMOR 27 TAHUN 2022 TENTANG PELINDUNGAN DATA PRIBADI. (2022).

UNDANG-UNDANG REPUBLIK INDONESIA NOMOR 39 TAHUN 1999 TENTANG HAK ASASI MANUSIA. (1999).

Yudistira, M., & Ramadani. (2023). *Jurnal Hukum, 13 Juli "TINJAUAN YURIDIS TERHADAP EFEKTIVITAS PENANGANAN KEJAHATAN SIBER TERKAIT PENCURIAN DATA PRIBADI MENURUT UNDANG-UNDANG NO. 27 TAHUN 2022 OLEH KOMINFO" bab Kesimpulan*. *5*, 3813–3814. https://doi.org/10.31933/unesrev.v5i4