Interdisciplinary Explorations in Research Journal (IERJ)
Vol. 3, Nomor 2 (Mei-Agustus, 2025), pp. 553-558
E-ISSN: 3032-1069

TINJAUAN YURIDIS TENTANG KEBOCORAN DATA *SUBSCRIBER IDENTITY MODULE* YANG DIRETAS DARI KEMENTERIAN KOMUNIKASI DAN DIGITAL

Ragil Anggriani[1], Muhammad Mashuri[2], Humiati[3]
[1,2,3]*Universitas Merdeka Pasuruan, Indonesia*
Email: ragilanggriani13@gmail.com[1], muh.mashuri86@gmail.com[2], humiatiariyono@gmail.com[3]

Received 18-04-2025| Revised 20-05-2025 | Accepted 28-06-2025

ABSTRACT
Cyberattacks that resulted in the loss of sensitive personal data have raised doubts in Indonesian society about the effectiveness of the existing data protection system. This study examines the legal liability of the Ministry of Communications and Digital Affairs with regard to the incident and analyzes the enforcement mechanisms within the framework of applicable legal provisions. The right to privacy is one of the fundamental human rights and must be guaranteed by the state in accordance with Article 28G, Paragraph (1) of the Constitution of the Republic of Indonesia of 1945. The protection of personal data is of central importance, as misuse can cause both material and immaterial harm not only to the affected individual but also to the institutions processing the data. This study is based on a normative legal methodology, applying a legal doctrine and case-based approach. The results reveal weaknesses in the existing cybersecurity framework, indicating inadequate implementation of data protection measures. In addition, legal accountability is problematic in practice, which underlines the need for action regarding stricter regulation and more efficient law enforcement..
Keyword: *data leaks, personal data protection, hacking.*

ABSTRAK
Serangan siber yang mengakibatkan hilangnya data pribadi yang sensitif telah menimbulkan keraguan di masyarakat Indonesia tentang efektivitas sistem perlindungan data yang ada. Penelitian ini mengkaji tanggung jawab hukum Kementerian Komunikasi dan Digital terkait insiden tersebut dan menganalisis mekanisme penegakan hukum dalam kerangka ketentuan hukum yang berlaku. Hak atas privasi merupakan salah satu hak asasi manusia yang fundamental dan harus dijamin oleh negara sesuai dengan Pasal 28G, Ayat (1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945. Perlindungan data pribadi menjadi sangat penting, karena penyalahgunaan dapat menyebabkan kerugian baik materiil maupun immaterial tidak hanya bagi individu yang terkena dampak tetapi juga bagi lembaga yang memproses data. Penelitian ini didasarkan pada metodologi hukum normatif, dengan menerapkan doktrin hukum dan pendekatan berbasis kasus. Hasil penelitian mengungkap kelemahan dalam kerangka keamanan siber yang ada, yang menunjukkan implementasi langkah-langkah perlindungan data yang tidak memadai. Selain itu, akuntabilitas hukum bermasalah dalam praktik, yang menggarisbawahi perlunya tindakan mengenai regulasi yang lebih ketat dan penegakan hukum yang lebih efisien.
Kata Kunci: kebocoran data, perlindungan data pribadi, peretasan.

PENDAHULUAN

Negara Republik Indonesia berlandaskan pada asas hukum. Berdasarkan Pasal 1 Ayat 3 Undang-Undang Dasar 1945, semua lembaga negara wajib menegakkan hukum secara menyeluruh untuk melindungi hak asasi warga negara, termasuk hak atas privasi dan perlindungan data pribadi.[1] Transformasi digital tidak hanya membawa kemajuan signifikan dalam teknologi informasi dan komunikasi, tetapi juga risiko yang cukup besar terutama yang berkaitan dengan perlindungan data pribadi. Kasus yang paling mengkhawatirkan adalah kebocoran data registrasi kartu SIM pada tahun 2022, yang menimbulkan kekhawatiran besar di masyarakat. Dalam konteks ini, seorang pengguna anonim dengan nama samaran "*Bjorka*" menawarkan data 1,3 miliar pengguna kartu SIM untuk dijual di web gelap. Paket data tersebut terdiri dari 87 *gigabyte* dan ditawarkan seharga $50.000, setara dengan sekitar 745 juta rupiah.[2]

Di antara informasi yang dibobol adalah nomor telepon seluler dan nomor induk kependudukan (NIK), yang seharusnya diperlakukan dengan sangat rahasia oleh negara, khususnya Kementerian Komunikasi dan Digital (Komdigi). Meskipun Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) memberikan dasar hukum yang kuat, masih terdapat perbedaan yang signifikan antara persyaratan hukum dan pelaksanaannya di lapangan. Pada kuartal ketiga tahun 2022, Indonesia menduduki peringkat ketiga di dunia dalam hal pelanggaran data yang dilaporkan, dengan total 12.742.031 akun pengguna yang terdampak.[3] Hal ini menyoroti kurangnya efektivitas mekanisme keamanan dan penegakan hukum yang diterapkan oleh lembaga pemerintah.

Menurut Hadjon, perlindungan hukum dapat dibagi menjadi dua yaitu perlindungan preventif dan perlindungan represif.[4] Hetty Hasanah menegaskan pentingnya perlindungan hukum untuk memberikan kepastian hukum bagi mereka yang terdampak pelanggaran hukum. Undang-Undang Perlindungan Data Pribadi (UU PDP) yang disahkan pada tahun 2022, berfungsi sebagai kerangka hukum yang komprehensif untuk menutup celah regulasi yang ada pada ketentuan sebelumnya,

[1] B. Hestu Cipto Handoyo, *Hukum Tata Negara, Kewarganegaraan dan Hak Asasi Manusia, Memahami Proses Konsolidasi Sistem Demokrasi di Indonesia*, (Yogyakarta: Universitas Atma Jaya Press, 2003); hal. 12.

[2] https://www.pinterpolitik.com/in-depth/sim-card-bocor-kominfo-bersalah/, diakses pada tanggal 5 Juni 2025.

[3] Kasus Kebocoran Data di Indonesia Melonjak 143% pada Kuartal II 2022, diakses pada tanggal 5 Juni 2025.

[4] Sudrajat Tedi dan Endra Wijaya; *Perlindungan Hukum Terhadap Tindakan Pemerintahan*; (Jakarta : Sinar Grafika, 2020); hal 102.

yakni UU ITE, PP No. 71 Tahun 2019, dan Permenkominfo No. 20 Tahun 2016.[5]

Penelitian ini berfokus pada tanggung jawab hukum Komdigi sebagai pengawas publik data pribadi terkait kebocoran data kartu SIM, serta pada penilaian efektivitas sanksi hukum dalam menangani insiden ini. Penelitian ini menggunakan metode hukum normatif yang menggabungkan pendekatan perundang-undangan dan pendekatan konseptual. Penelitian ini didasarkan pada data sekunder yang diperoleh dari sumber hukum primer (seperti Undang-Undang Dasar Republik Indonesia Tahun 1945, Undang-Undang Perlindungan Data, Undang-Undang ITE, Peraturan No. 71/2019, dan Permenkominfo No. 20/2016), sumber hukum sekunder (termasuk literatur akademis dan jurnal hukum), dan sumber hukum tersier (seperti kamus dan ensiklopedia hukum).[6] Analisis dilakukan secara kualitatif dengan metode interpretasi normative.

ANALISIS DAN PEMBAHASAN

1. Komdigi sebagai Pengendali Data dan Tanggung Jawab Hukumnya

Berdasarkan Pasal 1 Angka 4 Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), Kementerian Komunikasi dan Digital (Komdigi) tergolong sebagai entitas pengolah data di sektor publik. Komdigi bertanggung jawab secara tunggal atau bersama-sama untuk menentukan tujuan dan cara pengolahan data pribadi.[7] Dalam perannya ini, Komdigi secara hukum berkewajiban untuk memastikan keamanan data yang diolah dan mencegah pengungkapan yang tidak sah.

Berdasarkan Pasal 16(2)(e) Undang-Undang Perlindungan Data Pribadi, pengawas data wajib melindungi data pribadi dari akses yang tidak sah, pengungkapan yang melanggar hukum, penyalahgunaan, kehilangan, dan kerusakan. Jika terjadi pelanggaran data, mereka harus memberikan pemberitahuan tertulis kepada pihak yang terkena dampak dalam waktu tiga hingga dua jam.[8]

Insiden kebocoran data kartu SIM pada September 2022 menyoroti penerapan kewajiban hukum yang tidak efektif. Informasi pribadi seperti nomor telepon seluler dan nomor identifikasi nasional (NIK) dari total 1,3 miliar data dipublikasikan dan ditawarkan untuk dijual melalui forum darknet oleh pengguna yang menggunakan nama samaran "*Bjorka*". Pemeriksaan acak oleh pakar keamanan TI juga mengonfirmasi bahwa banyak data yang dipublikasikan adalah

[5] Dade, L. L., Waha, C. J., Nachrawy, N., *Kajian Yuridis Tentang Tindak Pidana Penyebaran Data Pribadi Melalui Internet (Doxing) Di Indonesia. LEX PRIVATUM*, Vol.13, No.3, 2024, hal.5.

[6] Muhaimin; *Metode Penelitian Hukum*; (Mataram: Mataram University Press, 2020); hal.64.

[7] Pasal 1 Angka 4 Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi.

[8] Pasal 46 Ayat (1) huruf e Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi.

asli dan masih aktif.[9]

Dari sudut pandang hukum, insiden ini termasuk dalam definisi pelanggaran perlindungan data sebagaimana didefinisikan dalam Pasal 1(25) Undang-Undang Perlindungan Data, karena melibatkan pelanggaran keamanan yang mengakibatkan akses, pengungkapan, penghapusan, atau perubahan data pribadi yang tidak sah. Namun, tidak ada informasi yang tersedia untuk umum mengenai penerapan sanksi administratif berdasarkan Pasal 57 dan 58 Undang-Undang Perlindungan Data yang telah diungkapkan kepada otoritas yang berwenang. Hal ini menyoroti kurangnya penegakan persyaratan hukum, meskipun insiden tersebut memenuhi syarat sebagai pelanggaran keamanan dan pemberitahuan yang terlambat.

2. Penegakan Hukum dalam Kebocoran Data, Tantangan dan Ketidakefektifan

Sebelum Undang-Undang Perlindungan Data Pribadi (UU PDP) disahkan, berbagai regulasi sektoral seperti UU ITE, Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PSTE), dan Permenkominfo No. 20 Tahun 2016 mengatur penanganan data pribadi. Namun, regulasi tersebut belum memiliki definisi yang jelas tentang istilah tersebut maupun sanksi yang konkret atas pelanggaran perlindungan data.[10]

Misalnya, Pasal 14 ayat (5) Peraturan Pemerintah Nomor 71 Tahun 2019 hanya mewajibkan penyelenggara sistem elektronik (PSE) untuk memberikan pemberitahuan tertulis apabila terjadi pelanggaran perlindungan data, tetapi tidak memuat sanksi tegas atas pelanggaran tersebut. Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 juga hanya mengatur tindakan administratif seperti peringatan, penghentian sementara, atau pencabutan izin penyelenggaraan.[11]

Dengan memberlakukan UU PDP, pemerintah berupaya menutup celah hukum yang ada. Namun, hingga kini belum ada penyidikan maupun tuntutan administratif maupun perdata yang dilakukan terhadap Komdigi terkait kebocoran data kartu SIM tersebut, meskipun Pasal 12 UU PDP secara tegas menjamin hak ganti rugi kepada pihak yang terdampak.[12]

---

[9] https://www.kompas.com/tren/read/2022/09/02/083741365/ramai-soal-dugaan-13-miliar-data-sim-card-bocor-ini-analisis-pakar?page=all#page2, diakses pada tanggal 5 Juni 2025.

[10] Dade, L. L., Waha, C. J., Nachrawy, N., *Kajian Yuridis Tentang Tindak Pidana Penyebaran Data Pribadi Melalui Internet (Doxing) Di Indonesia. LEX PRIVATUM*, Vol.13, No.3, 2024, hal.5.

[11] Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 20 Tahun 2016 Tentang Perlindungan Data Pribadi Dalam Sistem Elektronik.

[12] Pasal 12 Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi

3. Dampak Hukum, Ekonomi dan Sosial atas Kebocoran Data

Hilangnya data pribadi tidak hanya merupakan pelanggaran hukum yang berlaku, tetapi juga memiliki konsekuensi ekonomi dan sosial yang luas. Individu yang terdampak berisiko lebih tinggi menjadi korban penipuan, pencurian identitas, perundungan siber, dan bentuk kejahatan siber lainnya. Lebih jauh lagi, *doxing* (publikasi informasi pribadi yang tidak sah oleh pihak ketiga) sering terjadi setelah pelanggaran data tersebut.[13]

Di bidang hukum pidana, pelanggaran hak pribadi warga negara juga dapat dikenakan sanksi. Hal ini diatur dalam Pasal 65 ayat (1) Undang-Undang Perlindungan Data Pribadi, yang melarang pengumpulan atau penggunaan data pribadi secara tidak sah untuk keuntungan pribadi atau pihak ketiga.[14]

Namun, tindakan efektif terhadap pelanggaran tersebut sangat terhambat oleh terbatasnya kesadaran digital di kalangan masyarakat, infrastruktur keamanan siber yang tidak memadai, dan kurangnya badan independen untuk memantau perlindungan data pribadi.

KESIMPULAN

Peristiwa pencurian data akibat peretasan registrasi kartu SIM pada tahun 2022 lalu jelas menunjukkan bahwa lembaga negara, khususnya Kementerian Komunikasi dan Digital (Komdigi), sebagai lembaga yang bertanggung jawab, telah gagal melindungi data pribadi. Tanggung jawab hukum Komdigi secara jelas tertuang dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Undang-undang ini mewajibkan pengawas data untuk memastikan keamanan data, melaporkan pelanggaran data dalam waktu 3x24 jam, dan memulihkan hak-hak subjek data.

Namun, dalam praktiknya, terdapat kesenjangan yang jelas antara ketentuan hukum dan pelaksanaannya. Penuntutan atas penyalahgunaan data sejauh ini belum memadai, dan kurangnya informasi yang jelas tentang sanksi administratif atau ganti rugi perdata yang dijatuhkan menggarisbawahi lemahnya daya penegakan hukum baru tersebut. Kegagalan untuk membentuk lembaga pengawas perlindungan data yang independen, sebagaimana diatur dalam UU PDP, semakin memperburuk perlindungan hukum yang memang sudah tidak memadai.

Studi ini menggarisbawahi urgensi untuk segera mendirikan lembaga pengawasan perlindungan data pribadi yang independen, memperketat sanksi atas pelanggaran ketentuan perlindungan data pribadi, dan memperkuat literasi digital

[13] Oktaviani, S., Dewata, Y. J., & Fadlian, A, *Pertanggung Jawaban Pidana Kebocoran Data BPJS dalam Perspektif UU ITE, De Juncto Delicti: Journal Of Law*, Vol.1, No.2, hal.153.

[14] Pasal 65 Ayat (1) Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi.

masyarakat guna menjamin perlindungan data pribadi yang efektif dan menyeluruh di Indonesia.

DAFTAR PUSTAKA

Buku

B. Hestu Cipto Handoyo, Hukum Tata Negara, Kewarganegaraan dan Hak Asasi Manusia, Memahami Proses Konsolidasi Sistem Demokrasi di Indonesia, (Yogyakarta: Universitas Atma Jaya Press, 2003); hal. 12.

Muhaimin; Metode Penelitian Hukum; (Mataram: Mataram University Press, 2020); hal.64.

Sudrajat Tedi dan Endra Wijaya; Perlindungan Hukum Terhadap Tindakan Pemerintahan; (Jakarta : Sinar Grafika, 2020); hal 102.

Jurnal

Dade, L. L., Waha, C. J., Nachrawy, N., "Kajian Yuridis Tentang Tindak Pidana Penyebaran Data Pribadi Melalui Internet (*Doxing*) Di Indonesia". *LEX PRIVATUM*, Vol.13, No.3, 2024, hal.5.

Oktaviani, S., Dewata, Y. J., & Fadlian, A, "Pertanggung Jawaban Pidana Kebocoran Data BPJS dalam Perspektif UU ITE", *De Juncto Delicti: Journal Of Law*, Vol.1, No.2, hal.153.

Peraturan Perundang-Undangan

Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi Pasal 1 Angka 4.

_____, Pasal 12.

_____, Pasal 46 Ayat (1) huruf e.

_____, Pasal 65 Ayat (1).

Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 20 Tahun 2016 Tentang Perlindungan Data Pribadi Dalam Sistem Elektronik.

Website

https://www.pinterpolitik.com/in-depth/sim-card-bocor-kominfo-bersalah/, diakses pada tanggal 5 Juni 2025.

https://www.kompas.com/tren/read/2022/09/02/083741365/ramai-soal-dugaan-13-miliar-data-sim-card-bocor-ini-analisis-pakar?page=all#page2, diakses pada tanggal 5 Juni 2025.

Kasus Kebocoran Data di Indonesia Melonjak 143% pada Kuartal II 2022, diakses pada tanggal 5 Juni 2025.