Journal of Innovative and Creativity
Journal Homepage: https://joecy.org/index.php/joecy
e-mail: journaljoecy@gmail.com

Faculty of Education
University of Pahlawan Tuanku Tambusai
ISSN 2775-771X (Online)
ISSN 2962-570X (Printed)
5 (2) 2025, Page: 18420-18430

Implikasi Hukum Kebocoran Data Pribadi oleh Pemerintah terhadap Hak Asasi Manusia: Perspektif Hukum Pidana

Ridwan Rangkuti [1], Muhammad Faisal[2]
[1]Universitas Muhammadiyah Tapanuli Selatan
[2]Universitas Muhammadiyah Tapanuli Selatan

Corresponding Author: rangkutiridwan7@gmail.com[1] falsharahap@gmail.com[2]

Published: August , 2025

ABSTRAK

Transformasi digital dalam tata kelola pemerintahan telah menjadikan data pribadi warga negara sebagai aset strategis dalam penyelenggaraan pelayanan publik. Namun, lemahnya sistem perlindungan data di lingkungan institusi negara telah menyebabkan kebocoran informasi berskala besar, sebagaimana terungkap dalam kasus BPJS Kesehatan, PeduliLindungi, dan Pusat Data Nasional. Penelitian ini bertujuan untuk menganalisis implikasi hukum dari kebocoran data pribadi oleh instansi pemerintah terhadap perlindungan hak asasi manusia, dengan menekankan pada peran hukum pidana sebagai instrumen akuntabilitas negara. Penelitian ini merupakan penelitian hukum normatif yang menelaah norma-norma hukum positif, asas hukum, dan doktrin dalam sistem hukum pidana nasional. Pendekatan yang digunakan bersifat doktrinal dan konseptual, dengan menitikberatkan pada interpretasi sistematik dan teleologis terhadap Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi dan norma-norma hukum HAM, baik nasional maupun internasional. Hasil penelitian menunjukkan bahwa belum terdapat pengaturan eksplisit mengenai pertanggungjawaban pidana institusi negara atas kebocoran data pribadi dalam sistem hukum Indonesia. Ketentuan pidana yang ada masih terbatas pada subjek hukum korporasi privat dan individu, sehingga menciptakan kekosongan hukum ketika pelaku adalah badan publik. Ketiadaan mekanisme akuntabilitas pidana terhadap negara melemahkan fungsi hukum pidana sebagai sarana penegakan keadilan dan perlindungan HAM digital. Oleh karena itu, diperlukan reformulasi norma hukum pidana yang memasukkan lembaga negara sebagai subjek hukum pidana, pembentukan lembaga pengawas independen yang efektif, serta penguatan mekanisme sanksi terhadap kelalaian struktural institusi negara dalam pengelolaan data pribadi.

Keywords: Kebocoran Data Pribadi, Pemerintah, Hak Asasi manusia, Hukum Pidana

© The Author(s). 2021 Open Access This article is licensed under a Creative Commons Atibution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0

PENDAHULUAN

Revolusi digital telah mengubah pola hubungan antara negara dan warganya. Informasi pribadi tidak lagi disimpan secara manual, melainkan dikumpulkan, diproses, dan disimpan melalui sistem digital oleh institusi pemerintah dalam berbagai sektor pelayanan publik. Identitas individu kini bergantung pada infrastruktur data yang dimiliki negara, menjadikan data pribadi sebagai instrumen administratif dan kontrol sosial yang sangat vital (Solove, 2008).

Transformasi digital administrasi publik telah memasuki fase krusial di negara-negara modern, termasuk Indonesia, di mana data pribadi warga menjadi aset utama dalam proses penyelenggaraan layanan pemerintahan. Data tersebut dikelola secara elektronik dan digunakan untuk berbagai fungsi strategis, seperti sistem Kependudukan (Dukcapil), pelayanan kesehatan (BPJS), hingga layanan imigrasi. Keberadaan infrastruktur semacam Pusat Data Nasional (PDN) menandai intensifikasi konsolidasi data di tingkat nasional (Tommy & Nasution, 2025).

Fenomena kebocoran data pribadi telah diidentifikasi sebagai bentuk pelanggaran HAM digital yang tersembunyi (*invisible violation*)—dimana dampaknya tidak segera terlihat fisiknya, tetapi mencederai

hak atas identitas, privasi, dan keamanan digital individu (Zuboff, 2019). Negara sebagai penyelenggara pelayanan publik direntangkan antara kewajiban untuk mengelola data dan kewajiban etik serta hukum untuk menjaganya secara aman. Ketika negara gagal melindungi data tersebut, maka legitimasi negara sebagai pelindung hak warga menjadi dipertanyakan (Foucault, 1977).

Hak atas privasi yang melekat sebagai bagian dari hak asasi manusia telah mendapat pengakuan universal dalam berbagai instrumen internasional, seperti Pasal 12 *Universal Declaration of Human Rights* dan Pasal 17 *International Covenant on Civil and Political Rights*. Dalam konteks nasional, hak ini dijamin melalui Pasal 28G ayat (1) UUD 1945. Namun, jaminan konstitusional tersebut belum sepenuhnya diiringi dengan sistem perlindungan hukum yang operasional dan efektif, khususnya ketika pelanggaran dilakukan oleh institusi negara sendiri (Greenleaf, 2018).

Ketergantungan terhadap sistem digital menempatkan masyarakat pada posisi rentan. Pengumpulan data yang masif tanpa transparansi mekanisme perlindungan mengakibatkan munculnya asimetri informasi antara negara dan warga. Ketika kebocoran data terjadi, beban risiko ditanggung oleh masyarakat sebagai subjek data, sementara mekanisme pertanggungjawaban negara seringkali tidak berjalan efektif (Muryani & Wiraguna, 2024). Kondisi ini mengindikasikan adanya ketimpangan struktural dalam perlindungan hak atas privasi, yang justru terancam oleh penyelenggara negara itu sendiri.

Berbagai studi empiris telah membuktikan lemahnya tata kelola keamanan data publik. Kebocoran data BPJS Kesehatan yang mencakup 279 juta peserta menggambarkan kegagalan sistem Perlindungan Data Pribadi (Sorisa, Kiareni, & Parhusip, 2024). Evaluasi audit forensik menemukan bahwa enkripsi dan kontrol akses tidak diterapkan secara memadai, sementara mekanisme deteksi dini tidak pernah dioperasionalkan. Insiden perilaku serupa terjadi pada kebocoran sistem PeduliLindungi dan MyPertamina yang memunculkan data sensitif warga dijual di forum gelap (Al Baihaqy, Fatimah, & Wicaksono, 2025).

Insiden tersebut disusul dengan kebocoran data pengguna aplikasi PeduliLindungi dan MyPertamina, yang menandai lemahnya proteksi pada aplikasi milik pemerintah yang secara langsung mengakses dan menyimpan data pribadi warga. Dalam studi yang dilakukan oleh Al Baihaqy, Fatimah, dan Wicaksono (2025), diketahui bahwa pola ancaman siber yang terjadi pada sistem pemerintah mencerminkan absennya kebijakan teknis yang mendetail terkait pemrosesan dan penyimpanan data. Serangan ransomware terhadap Pusat Data Nasional (PDN) pada pertengahan 2024 menjadi puncak krisis keamanan siber, ketika lebih dari 282 lembaga pemerintahan lumpuh total akibat sistem terenkripsi dan tidak memiliki cadangan data terpadu.

Puncaknya muncul pada serangan ransomware terhadap Pusat Data Nasional (PDN) dalam bentuk Brain Cipher (varian LockBit 3.0) pada tanggal 17–20 Juni 2024. BSSN melaporkan bahwa sistem keamanan Windows Defender telah dinonaktifkan sejak 17 Juni pukul 23.15 WIB; data pada 239 institucipemerintah dan daerah disandera mulai 20 Juni 2024, dengan permintaan tebusan sebesar 8 juta dolar AS (~Rp 131,2 miliar) (Tempo.co, 2 Juli 2024; Kompas, 25 Juni 2024; CSIRT, 2024)

Investigasi lanjutan mengungkap bahwa hanya 2 % data yang sempat diback-up, sehingga upaya pemulihan gagal dilakukan dan mayoritas sistem tidak dapat diakses (Tempo.co, 27 Juni 2024). Gangguan layanan menyebabkan antrian panjang di imigrasi, perlambatan pelayanan publik, dan penurunan kepercayaan publik terhadap legitimasi pemerintah sebagai pengelola data (Katadata, 2024; Kompas, 2024). Kelangkaan cadangan dan lemahnya prosedur keamanan menunjukkan ketidaksiapan institusional di internal Kominfo dan Telkomsigma sebagai pengelola PDN. Banyak pengguna sistem mengandalkan pengamanan minimal seperti antivirus desktop (SMADAV) tanpa kebijakan backup sistemik (Reddit user reports)

Krisis tersebut tidak hanya mengganggu layanan administrasi publik, tetapi juga mengancam hak-hak sipil dan politik warga negara. Layanan seperti pendidikan tinggi, sistem perpajakan, e-budgeting, hingga basis data pemilu terganggu, sehingga menghambat akses terhadap layanan dasar yang dilindungi oleh negara. Studi kebijakan yang dilakukan oleh Tech For Good Institute (2024)

menunjukkan bahwa Indonesia termasuk dalam kelompok negara dengan indeks mitigasi risiko siber terendah di Asia Tenggara, akibat belum berfungsinya sistem pengawasan independen terhadap pengelolaan data publik.

Walaupun UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi telah diundangkan, efektivitasnya masih menjadi tanda tanya besar. Lembaga pengawas independen yang diamanatkan dalam undang-undang belum dibentuk secara definitif hingga tahun 2025, sehingga tidak tersedia entitas yang bertanggung jawab secara langsung terhadap dugaan pelanggaran yang dilakukan instansi pemerintah. Dalam penelitian yang dilakukan oleh Muryani dan Wiraguna (2024), disebutkan bahwa pelaksanaan UU PDP masih bersifat elitis dan tidak menyentuh akar masalah struktural berupa ketidaksiapan kelembagaan dan rendahnya budaya perlindungan privasi di kalangan birokrasi.

Dalam praktik penegakan hukum, belum pernah ditemukan satu pun kasus pidana yang menjerat institusi pemerintah sebagai pelaku kebocoran data. Hal ini mengindikasikan ketidakseimbangan (*inequality before the law*) sebagaimana ditemukan dalam evaluasi oleh Muryani dan Wiraguna (2024). Aparat penegak hukum tampak terjebak dilema antara independensi profesi dan tekanan institusional atas kasus yang melibatkan struktur pemerintahan (ICJR, 2023).

Implikasi kebocoran data melebihi sekadar masalah teknis atau administratif. Hak atas privasi, identitas digital, serta hak untuk tidak diperlakukan secara diskriminatif telah terancam secara nyata. Data seperti status kesehatan, preferensi politik, atau rekam transaksi dapat digunakan untuk profiling digital dan kriminalisasi berbasis metadata, terutama terhadap kelompok rentan (Amnesty Tech, 2022)

Ketiadaan akuntabilitas pidana terhadap institusi negara dalam kasus kebocoran data pribadi menimbulkan permasalahan serius dalam sistem hukum pidana nasional. Padahal, menurut teori pertanggungjawaban pidana korporasi, lembaga negara sebagai badan hukum publik dapat dimintakan tanggung jawab jika memenuhi unsur perbuatan melawan hukum, kesalahan, dan akibat yang ditimbulkan (Muladi, 2002). Dalam konteks ini, pertanggungjawaban pidana terhadap instansi pemerintah masih menjadi wilayah yang kurang tereksplorasi secara normatif dan empiris.

Permasalahan semakin kompleks ketika hak atas privasi dipertemukan dengan dimensi HAM. Kebocoran data yang menyebabkan diskriminasi, peretasan, dan penyalahgunaan identitas berdampak langsung terhadap kualitas hidup individu dan masyarakat. Studi komparatif oleh FRA (2020) menemukan bahwa negara-negara dengan tingkat pelanggaran data tinggi cenderung memiliki skor kepercayaan publik yang rendah terhadap pemerintah. Implikasi ini berkelindan dengan hak atas perlindungan hukum, kebebasan berekspresi, dan keamanan digital sebagai bagian dari hak asasi manusia di era teknologi.

Tumpang tindih antara norma hukum pidana, hukum administrasi, dan hukum perlindungan data menghadirkan tantangan metodologis dalam menentukan bentuk pertanggungjawaban yang tepat. Belum adanya preseden yuridis di Indonesia yang menetapkan instansi pemerintah sebagai pelaku tindak pidana data, menunjukkan bahwa terdapat kekosongan penerapan norma dalam lingkup hukum positif. Kelemahan ini berdampak pada potensi berkembangnya impunitas kelembagaan dalam pelanggaran hak privat warga negara.

Sistem hukum pidana nasional saat ini kurang mampu menghadapi pelanggaran oleh institusi publik yang bersifat sistemik. Pasal-pasal dalam UU PDP belum merumuskan dengan jelas tentang pertanggungjawaban pidana institusi pemerintah. Lembaga negara yang menjadi pengendali data utama seringkali tidak diawasi secara independen, sehingga akses keadilan menjadi terbatas (Teguh, 2023; ICJR, 2023)

Berdasarkan paparan tersebut, penelitian ini difokuskan pada upaya mengkaji bagaimana implikasi hukum dari kebocoran data pribadi oleh instansi pemerintah terhadap perlindungan hak asasi manusia, khususnya melalui perspektif hukum pidana sebagai instrumen akuntabilitas negara.

METODOLOGI PENELITIAN

Penelitian ini merupakan penelitian hukum normatif (*normative legal research*), yaitu suatu bentuk kajian yang menempatkan hukum sebagai suatu sistem norma yang otonom dan koheren, serta dianalisis melalui instrumen yuridis yang bersifat doktrinal. Dalam kerangka ini, hukum tidak dipandang sebagai gejala empiris, melainkan sebagai konstruksi sistematis yang harus dipahami melalui pendekatan tekstual, logis, dan sistematis terhadap produk hukum positif yang berlaku (Soekanto & Mamudji, 2001). Fokus utama terletak pada analisis terhadap norma-norma yang terkodifikasi, serta kekosongan, ketidakjelasan, atau tumpang tindih antar ketentuan hukum yang berlaku—dalam hal ini terkait tanggung jawab hukum pidana negara atas kebocoran data pribadi.

Jenis penelitian normatif dipilih karena persoalan yang dikaji dalam penelitian ini berakar pada problem normatif dan dogmatis, bukan semata pada realitas empiris. Permasalahan utama bukan pada "apakah" kebocoran data itu terjadi, melainkan "bagaimana" hukum pidana meresponsnya ketika pelaku yang bertanggung jawab adalah institusi negara. Perspektif ini membutuhkan analisis mendalam terhadap struktur perundang-undangan, asas hukum, dan teori pertanggungjawaban pidana yang selama ini lebih banyak diaplikasikan pada entitas privat atau individu.

Dalam konteks hukum Indonesia, kebocoran data pribadi yang dilakukan oleh institusi pemerintah belum secara eksplisit diatur sebagai tindak pidana dengan subjek hukum berupa badan publik. Hal ini menimbulkan *lacuna legis* atau kekosongan hukum, yang membutuhkan analisis doktrinal untuk mengidentifikasi kemungkinan reinterpretasi terhadap norma yang ada, serta usulan pembaruan hukum pidana nasional. Sebagaimana ditegaskan oleh Marzuki (2005), penelitian hukum normatif memiliki peran sentral dalam mengevaluasi dan membentuk sistem hukum agar mampu merespons perkembangan sosial dan teknologi secara progresif.

Pendekatan normatif relevan digunakan untuk menganalisis ketidakseimbangan antara norma HAM internasional—seperti hak atas privasi dan hak atas rasa aman digital—dengan pelaksanaan norma hukum nasional dalam konteks Indonesia. Ketika negara, melalui instrumen administratif dan teknologinya, lalai melindungi data warga, maka timbul pertanyaan normatif mengenai tanggung jawab pidana institusional yang belum terakomodasi dalam struktur hukum pidana nasional. Dalam hal ini, asas legalitas (nullum crimen sine lege) menjadi ujian serius ketika hukum yang ada tidak memuat ketentuan pidana yang memadai untuk pelanggaran oleh badan publik (Muladi & Arief, 1992).

Jenis penelitian ini dapat pula dikategorikan sebagai penelitian hukum normatif-progresif. Dalam pendekatan ini, hukum tidak semata-mata dipahami sebagai teks statis, melainkan sebagai sistem nilai yang berkembang dan harus adaptif terhadap kebutuhan perlindungan HAM di era digital (Satjipto Rahardjo, 2006). Oleh sebab itu, penelitian ini tidak berhenti pada evaluasi normatif terhadap UU PDP dan KUHP, tetapi juga mendorong rekonstruksi norma hukum pidana yang mampu menjangkau entitas negara sebagai subjek hukum secara lebih eksplisit.

Penggunaan jenis penelitian ini memungkinkan peneliti untuk menggali, menelaah, dan menafsirkan norma-norma hukum yang relevan dengan kasus kebocoran data pribadi oleh pemerintah melalui teknik argumentasi hukum, analisis sistematik, serta interpretasi teleologis terhadap prinsip-prinsip hukum yang berlaku. Penekanan diberikan pada interpretasi progresif dan sistematis, yakni bagaimana suatu norma dipahami dalam kerangka perlindungan hak asasi manusia secara substansial, serta dalam konteks transformasi hukum yang dipicu oleh perkembangan teknologi dan digitalisasi pelayanan publik.

Penelitian ini menggunakan tiga jenis bahan hukum:

1. Bahan hukum primer, yaitu peraturan perundang-undangan seperti:
   a. Undang-Undang Dasar Negara Republik Indonesia Tahun 1945
   b. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi

c. Kitab Undang-Undang Hukum Pidana (KUHP)
d. Instrumen HAM internasional: *Universal Declaration of Human Rights*, *International Covenant on Civil and Political Rights*

2. Bahan hukum sekunder, yaitu literatur akademik, hasil penelitian, dan jurnal ilmiah, seperti karya dari Zuboff (2019), Foucault (1977), dan publikasi dari Amnesty Tech, ICJR, serta jurnal hukum dan teknologi informasi.
3. Bahan hukum tersier, yaitu kamus hukum, ensiklopedia hukum, serta dokumen laporan media terpercaya (Tempo, Kompas, Katadata) yang digunakan untuk memperkuat konteks faktual kebocoran data.

Bahan hukum dikumpulkan melalui studi pustaka (*library research)* terhadap peraturan perundang-undangan, jurnal hukum nasional dan internasional, laporan lembaga riset, serta dokumentasi kasus kebocoran data yang telah terjadi. Teknik ini dilakukan secara sistematis untuk memastikan akurasi dan kredibilitas sumber.

Bahan hukum dianalisis menggunakan pendekatan deskriptif-kualitatif, yakni dengan cara menguraikan permasalahan hukum yang terjadi, mengidentifikasi celah hukum, dan mengkaji implikasi normatifnya. Analisis dilakukan secara deduktif, diawali dari asas dan norma hukum umum kemudian diturunkan pada persoalan khusus kebocoran data oleh institusi pemerintah. Selain itu, digunakan pula teknik *interpretasi sistematis dan teleologis*, guna memahami makna norma hukum secara menyeluruh dan sesuai dengan tujuan perlindungan HAM dalam era digital.

HASIL DAN PEMBAHASAN

Hak Asasi Manusia dan Data Pribadi Serta Keterkaitannya Dalam Konteks Hukum Digital

Hak Asasi Manusia merupakan hak yang melekat pada setiap individu sebagai manusia, bersifat universal, tidak dapat dicabut (*inalienable*), dan berdasar pada martabat manusia. HAM dijamin secara normatif melalui instrumen-instrumen internasional seperti *Universal Declaration of Human Rights* (UDHR, 1948) dan *International Covenant on Civil and Political Rights* (ICCPR, 1966). Pasal 12 UDHR dan Pasal 17 ICCPR mengatur hak atas privasi dan perlindungan terhadap gangguan sewenang-wenang terhadap kehidupan pribadi, rumah tangga, keluarga, dan komunikasi (UNHRC, 2018; Privacy International, 2025).

Hak atas privasi merupakan pilar penting bagi kebebasan individu dan nilai demokrasi. Asas ini memungkinkan seseorang berfungsi secara otonom tanpa intimidasi atau pemantauan yang tidak sah. Pelaksanaan hak atas privasi mendasari hak atas kebebasan berekspresi, kebebasan berkumpul, dan hak atas keamanan digital (Privacy International, 2025).

Data pribadi mencakup semua informasi yang dapat mengidentifikasi seseorang secara langsung atau tidak langsung—meliputi nama, NIK, alamat, riwayat kesehatan, data transaksi, dan metadata sebagaimana diatur dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Data tersebut menjadi representasi digital atas identitas seseorang dalam sistem administrasi publik dan teknologi informasi (Longstaff, 2024).

Dalam konteks digitalisasi administrasi publik, data pribadi bukan hanya komoditas administratif, melainkan aset identitas yang menyatu dengan hak-hak sipil warga negara. Pengolahan data dilakukan melalui pengumpulan, penyimpanan, pengubahan, dan distribusi melalui alat digital—mengharuskan adanya perlindungan hukum yang tidak hanya administratif, tetapi juga bersifat substantif (Longstaff, 2024; Droit-Humain, 2024).

Data pribadi mencakup semua informasi yang dapat mengidentifikasi seseorang secara langsung atau tidak langsung—meliputi nama, NIK, alamat, riwayat kesehatan, data transaksi, dan metadata sebagaimana diatur dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Data tersebut menjadi representasi digital atas identitas seseorang dalam sistem administrasi publik dan teknologi informasi (Longstaff, 2024).

Dalam konteks digitalisasi administrasi publik, data pribadi bukan hanya komoditas administratif, melainkan aset identitas yang menyatu dengan hak-hak sipil warga negara. Pengolahan data dilakukan melalui pengumpulan, penyimpanan, pengubahan, dan distribusi melalui alat digital—mengharuskan adanya perlindungan hukum yang tidak hanya administratif, tetapi juga bersifat substantif (Longstaff, 2024; Droit-Humain, 2024).

Transparansi dan akuntabilitas institusional menjadi krusial ketika negara bertindak sebagai pengendali data. Negara memiliki kewajiban untuk tidak hanya menghormati hak warga atas privasi, tetapi juga melindunginya dari penyalahgunaan internal atau eksternal (World Jurisprudence, 2025). Ketika negara gagal melindungi data warga, legitimasi negara sebagai institusi pelindung HAM dipertanyakan (Toronto Declaration, 2018).

Fragilitas sistem hukum pidana terhadap pelanggaran data oleh institusi publik menunjukkan bahwa keseimbangan antara perlindungan HAM dan pengelolaan data belum sepenuhnya dijamin. Ketika pelaku adalah entitas pemerintah itu sendiri, tidak ada norma eksplisit yang mengatur pertanggungjawaban pidana institusional. Ini menyebabkan ketidakcocokan antara norma HAM internasional dan hukum nasional, serta munculnya impunitas struktural (Teguh, 2023; ICJR, 2023).

Pengertian HAM dan data pribadi saling terintegrasi secara filosofis, normatif, dan operasional. Perlindungan data pribadi adalah bagian yang tidak terpisahkan dari pelaksanaan HAM di era digital. Pelanggaran data, terutama oleh negara, mencerminkan kegagalan negara memenuhi tanggung jawab konstitusional dan human rights standard. Reformasi hukum pidana yang inklusif perlu dirumuskan untuk memastikan negara tidak hanya subjek pengatur, tetapi juga subjek hukum yang dapat dituntut ketika terjadinya pelanggaran hak atas privasi warga negara.

Tanggung Jawab Pidana Institusional Negara

Dalam sistem pemerintahan modern, negara tidak hanya berperan sebagai regulator, tetapi juga bertindak sebagai pengendali utama terhadap data pribadi warganya. Posisi ini secara hukum ditegaskan dalam Pasal 1 angka 4 Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), yang menyebutkan bahwa institusi negara merupakan bagian dari pengendali data. Dengan demikian, negara memiliki dua lapis tanggung jawab: kewajiban hukum positif untuk melindungi data pribadi serta kewajiban moral untuk menjaga integritas hubungan antara negara dan warga negara dalam ruang digital. Ketika negara lalai atau gagal menjalankan fungsi ini, timbul implikasi serius terhadap legitimasi dan kredibilitas penyelenggara pemerintahan.

Kebocoran data pribadi dalam kasus BPJS, PeduliLindungi, hingga serangan terhadap Pusat Data Nasional (PDN) bukan hanya menunjukkan celah keamanan teknis, tetapi juga mencerminkan lemahnya akuntabilitas hukum negara. Fakta bahwa data yang dicuri menyangkut informasi sensitif seperti NIK, riwayat medis, hingga transaksi digital memperlihatkan betapa strategisnya peran negara sebagai pelindung hak digital warga. Dalam konteks ini, hak atas privasi sebagaimana diatur dalam Pasal 28G ayat (1) UUD 1945 serta dalam Pasal 17 International Covenant on Civil and Political Rights (ICCPR) telah terancam secara struktural.

Hukum pidana Indonesia belum secara eksplisit mengakui negara atau institusi pemerintahan sebagai subjek hukum pidana (legal subject). KUHP maupun UU PDP belum merumuskan secara operasional bagaimana pertanggungjawaban pidana dapat dikenakan kepada entitas publik apabila terjadi kelalaian atau pelanggaran dalam perlindungan data. Model pertanggungjawaban pidana korporasi yang selama ini diakui (vide Pasal 45 UU ITE dan Pasal 118 UU PDP) umumnya diarahkan pada entitas swasta.

Ketiadaan mekanisme pertanggungjawaban pidana negara menciptakan ketimpangan fundamental dalam prinsip *equality before the law*. Ketika perusahaan swasta dapat dipidana karena kelalaian mengelola data pengguna, sedangkan institusi negara tidak dikenai mekanisme hukum serupa, maka hukum kehilangan prinsip keadilan substansial. Evaluasi oleh Muryani dan Wiraguna (2024) menegaskan bahwa aparat penegak hukum kerap menghadapi dilema etis dan tekanan struktural

dalam menangani kasus yang melibatkan institusi pemerintahan, sehingga penegakan hukum cenderung bersifat diskriminatif.

Kebocoran data tidak hanya menimbulkan kerugian material dan teknis, tetapi juga berimplikasi pada pelanggaran hak asasi manusia, khususnya hak atas privasi, hak atas rasa aman, dan hak untuk tidak diperlakukan secara diskriminatif. Amnesty Tech (2022) menyoroti bahwa pelanggaran data digital merupakan bentuk *invisible violation*, karena dampaknya tidak langsung tampak secara fisik, namun dapat digunakan untuk profilisasi politik, komersial, dan bahkan kriminalisasi terhadap individu atau kelompok rentan.

Negara sebagai pelindung utama HAM memiliki tanggung jawab untuk menjamin akses keadilan atas pelanggaran tersebut. Namun dalam praktiknya, tidak tersedia mekanisme kompensasi atau restitusi bagi korban kebocoran data yang dilakukan oleh lembaga publik. Lembaga independen yang seharusnya dibentuk berdasarkan UU PDP belum efektif beroperasi, menyebabkan kekosongan pengawasan administratif maupun pengenaan sanksi pidana terhadap pelaku dari sektor negara.

Negara harus mampu menjawab kekosongan hukum dan menciptakan sistem pertanggungjawaban yang adil, maka diperlukan reformasi normatif terhadap hukum pidana Indonesia. Pertama, perluasan subjek hukum pidana harus secara eksplisit mencakup badan publik sebagai subjek hukum yang dapat dipidana. Model pertanggungjawaban institusional negara dapat mengacu pada prinsip *state accountability* dalam konteks pelanggaran HAM berat atau pada mekanisme pidana administratif di beberapa yurisdiksi Eropa.

Kedua, perlu dibentuk lembaga independen pengawas data yang memiliki kewenangan kuat, baik dalam pengawasan, penyidikan, maupun penindakan atas pelanggaran yang dilakukan oleh institusi negara. Ketiga, prosedur remediasi bagi warga sebagai korban kebocoran data harus dijamin, baik melalui jalur administratif, perdata, maupun pidana. Proses ini penting agar negara tidak hanya bertindak sebagai pengendali data, tetapi juga sebagai entitas yang bertanggung jawab secara hukum apabila terjadi kelalaian yang merugikan warga.

Implikasi Hukum Kebocoran Data Pribadi oleh Pemerintah terhadap Perlindungan Hak Asasi Manusia: Perspektif Hukum Pidana sebagai Instrumen Akuntabilitas

Seluruh aktivitas pelayanan publik seperti sistem kependudukan, kesehatan, keuangan, pendidikan, dan transportasi bergantung pada pengelolaan data pribadi secara elektronik. Dalam arsitektur ini, negara tidak hanya menjadi pengumpul data, tetapi juga pengendali dan penanggung jawab atas keamanan dan integritas informasi warga. Ketika data pribadi digunakan dalam skala besar untuk kebutuhan pelayanan publik, maka keamanan dan kerahasiaannya menjadi bagian yang tidak terpisahkan dari perlindungan hak-hak dasar manusia.

Ketika terjadi kebocoran data yang bersumber dari institusi pemerintah, tanggung jawab negara menjadi sorotan utama dalam aspek hukum dan HAM. Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, khususnya Pasal 28G ayat (1), telah menjamin hak setiap orang atas perlindungan diri pribadi dan rasa aman dari ancaman terhadap hak atas kebebasan dan integritas pribadinya. Jaminan ini diperkuat oleh Pasal 17 International Covenant on Civil and Political Rights (ICCPR), yang menegaskan larangan terhadap intervensi sewenang-wenang terhadap kehidupan pribadi, keluarga, komunikasi, dan kehormatan seseorang. Negara sebagai pelaku administrasi elektronik diwajibkan oleh hukum internasional maupun konstitusi nasional untuk menjamin bahwa informasi warga tidak bocor, tidak dimanipulasi, dan tidak disalahgunakan.

Absennya mekanisme pertanggungjawaban pidana terhadap institusi negara dalam kasus kebocoran data menciptakan kekosongan norma dalam sistem hukum nasional. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi memberikan ancaman pidana terhadap pelaku yang lalai atau menyalahgunakan data pribadi, namun fokus utamanya hanya pada subjek hukum korporasi privat dan individu. Tidak terdapat ketentuan eksplisit yang memposisikan institusi negara sebagai pelaku tindak pidana, meskipun secara faktual telah terjadi insiden sistemik yang

mengakibatkan terungkapnya data pribadi jutaan warga negara. Kondisi ini memunculkan ketidakseimbangan dalam asas kesetaraan di hadapan hukum serta mengaburkan fungsi hukum pidana sebagai alat kontrol sosial terhadap semua pelaku, termasuk aktor negara.

Penegakan hukum atas pelanggaran hak privasi yang dilakukan oleh lembaga pemerintah tidak pernah berhasil sampai pada ranah pidana. Pemerintah sebagai entitas struktural memiliki kekebalan informal dalam praktik hukum, karena tidak terdapat yurisdiksi pidana yang mampu memproses kelalaian institusional secara efektif. Hukum pidana nasional tidak memberikan ruang bagi pertanggungjawaban kolektif yang dapat dikenakan kepada lembaga negara, meskipun lembaga tersebut terbukti lalai dalam mengelola dan melindungi data warganya. Aspek ini menunjukkan bahwa sistem hukum masih bersifat asimetris dalam membedakan antara pelaku publik dan privat.

Hak atas privasi sebagai bagian dari hak asasi manusia terancam ketika data pribadi digunakan tanpa persetujuan, diakses secara ilegal, atau bahkan dijual di ruang gelap internet. Ketika negara sebagai pengendali data justru menjadi sumber kebocoran, maka terjadi disfungsi peran konstitusional negara dalam menjamin kebebasan pribadi dan rasa aman warganya. Amnesty Tech (2022) menilai bahwa pelanggaran data digital oleh aktor negara adalah bentuk pelanggaran HAM yang tidak terlihat secara fisik, tetapi berdampak jangka panjang pada kerentanan politik, ekonomi, dan sosial korban.

Hukum pidana memiliki potensi strategis sebagai instrumen untuk menciptakan akuntabilitas negara. Pertanggungjawaban pidana terhadap lembaga negara secara teoretik memungkinkan dengan mengadopsi model *corporate criminal liability* yang diperluas ke entitas publik. Prinsip pertanggungjawaban dapat diarahkan pada kebijakan internal, sistem pengawasan yang lemah, serta kegagalan sistemik dalam pencegahan pelanggaran. Beberapa sistem hukum di Eropa telah mengenali bentuk pertanggungjawaban ini untuk lembaga publik dalam kasus pelanggaran HAM administratif. Adaptasi model ini ke dalam sistem hukum Indonesia menjadi relevan mengingat tingginya eskalasi risiko kebocoran data pada sektor publik.

Instrumen hukum pidana tidak hanya berfungsi menjerakan pelaku, tetapi juga mengoreksi struktur kelembagaan yang lemah. Sanksi pidana terhadap lembaga negara yang lalai dapat disusun dalam bentuk pidana denda institusional, pengurangan anggaran, pembubaran unit kerja, atau pelimpahan wewenang kepada lembaga lain. Pendekatan ini memperkuat fungsi hukum pidana sebagai kontrol vertikal terhadap kekuasaan negara dalam sistem demokrasi. Model ini juga menunjukkan bahwa hukum tidak bersifat eksklusif terhadap warga, tetapi bersifat imparsial terhadap semua bentuk pelanggaran, termasuk oleh negara terhadap rakyatnya.

KESIMPULAN

Kebocoran data pribadi oleh institusi pemerintah merupakan bentuk kegagalan negara dalam memenuhi kewajiban konstitusional dan internasional untuk melindungi hak asasi manusia, khususnya hak atas privasi dan rasa aman digital. Meskipun digitalisasi pelayanan publik merupakan keniscayaan dalam era teknologi, pengelolaan data pribadi yang dilakukan tanpa standar perlindungan hukum yang memadai akan berakibat pada terjadinya pelanggaran sistemik terhadap martabat dan hak-hak dasar warga negara.

Hukum pidana nasional belum secara eksplisit mengatur pertanggungjawaban pidana terhadap institusi negara atas kelalaian yang menyebabkan kebocoran data. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi cenderung mengarahkan sanksi pidana kepada individu dan korporasi privat, sehingga negara sebagai subjek hukum kolektif belum dapat disentuh secara langsung oleh instrumen hukum pidana. Ketimpangan ini menimbulkan ketidakadilan struktural dan mengaburkan prinsip persamaan di hadapan hukum.

Ketiadaan mekanisme pidana yang menjangkau aktor negara mengakibatkan tidak tercapainya fungsi hukum pidana sebagai sarana pengendali sosial yang efektif. Akuntabilitas negara atas pelanggaran HAM digital tidak dapat ditegakkan melalui jalur hukum represif, meskipun dampak dari kebocoran

data sangat signifikan dan menyasar kelompok warga secara luas. Kondisi ini memperlihatkan kelemahan mendasar dalam sistem perundang-undangan nasional dalam menghadapi tantangan perlindungan HAM di era digital.

Instrumen hukum pidana semestinya digunakan tidak hanya untuk menjatuhi sanksi terhadap individu, tetapi juga untuk menegakkan tanggung jawab kolektif lembaga negara yang terbukti lalai atau abai dalam menjalankan kewajiban perlindungan data. Penegakan hukum pidana terhadap negara penting untuk memulihkan hak-hak korban, mengembalikan kepercayaan publik, dan memastikan negara tidak dikecualikan dari sistem keadilan.

SARAN

Berdasarkan hasil dan pembahasan serta kesimpulan penelitian maka dapat diperoleh saran penelitian, yaitu:

1. Reformulasi Norma Pidana dalam UU PDP; Ketentuan pidana dalam Undang-Undang Perlindungan Data Pribadi perlu direvisi untuk secara eksplisit memasukkan institusi pemerintah sebagai subjek hukum pidana. Hal ini penting guna menutup celah hukum dan memastikan kesetaraan pertanggungjawaban antara sektor publik dan privat.
2. Penguatan Mekanisme Akuntabilitas Institusional; Diperlukan mekanisme pertanggungjawaban pidana institusional, melalui konsep strict liability atau vicarious liability, terhadap lembaga negara yang lalai dalam perlindungan data pribadi. Penegakan dapat diformulasikan dalam bentuk pidana denda institusional, pembatasan operasional, atau sanksi struktural administratif.
3. Pembentukan Lembaga Independen Penegak UU PDP; Sebagaimana diamanatkan dalam UU PDP, pembentukan lembaga pengawas independen harus segera direalisasikan dengan kewenangan penegakan hukum yang kuat, termasuk wewenang untuk melakukan penyidikan, pemantauan, dan pengajuan tuntutan pidana terhadap pelanggaran oleh lembaga pemerintah.
4. Penyusunan Pedoman Teknis Perlindungan HAM Digital; Pemerintah bersama Komnas HAM dan BSSN perlu menyusun pedoman nasional yang mengintegrasikan prinsip-prinsip HAM dalam pengelolaan data pribadi, termasuk tanggung jawab pidana apabila terjadi kelalaian. Pedoman ini harus menjadi acuan hukum sektoral dan kebijakan internal lembaga negara.
5. Peningkatan Literasi Digital Hukum di Lingkungan Pemerintah; Perlu diselenggarakan pelatihan reguler mengenai perlindungan data pribadi dan hukum HAM digital bagi seluruh aparatur sipil negara yang terlibat dalam pengelolaan data. Peningkatan kapasitas ini bertujuan untuk mencegah pelanggaran yang disebabkan oleh ketidaktahuan atau kesalahan prosedural.

DAFTAR PUSTAKA

Al Baihaqy, A., Fatimah, N., & Wicaksono, B. (2025). *Krisis Siber Nasional dan Revisi Paradigma Keamanan Digital Pemerintah*. Jurnal Keamanan Siber Nasional, 4(2), 103–127.

Amnesty Tech. (2022). *Surveillance, profiling, and discrimination in digital ecosystems*. London: Amnesty International.

Apex Judgments. (2024). *Understanding privacy in international law: A comprehensive guide*. The Hague: Apex Publishers.

Borgesius, F. Z., Asghari, H., Bangma, N., & Hoepman, J.-H. (2024). The GDPR's rules on data breaches: Analysing their rationales and effects. *arXiv preprint*.

Chairunnisa, S., Ramadhan, D., & Lestari, H. (2023). *Aspek Yuridis Perlindungan Data Pribadi dalam Pemerintahan Digital*. Jurnal Hukum & Masyarakat, 15(1), 55–76.

Council of Europe's Convention 108. (2020). *Convention for the protection of individuals with regard to automatic processing of personal data*.

Droit-Humain. (2024). *Human rights and digital privacy: Protecting personal data in the modern age*. Paris: Droit-Humain Publishing.

Foucault, M. (1977). *Discipline and punish: The birth of the prison* (A. Sheridan, Trans.). New York: Pantheon Books.

FRA – European Union Agency for Fundamental Rights. (2020). *Data quality and the right to privacy*. Vienna: FRA.

Greenleaf, G. (2018). Global data privacy laws 2017: 120 national data privacy laws, including Indonesia's draft PDP law. *Privacy Laws & Business International Report*, 145, 10–13.

ICJR. (2023). *Evaluasi penegakan hukum pelanggaran data pribadi oleh institusi pemerintah*. Jakarta: Institute for Criminal Justice Reform.

Katadata. (2024). *Dampak kebocoran data PDN terhadap pelayanan publik*. Jakarta: Katadata Insight Center.

Kompas. (2024). *Data KPU dan Dukcapil Diduga Bocor, Publik Resah*. Kompas Investigasi.

Kompas. (2024). *Krisis kepercayaan publik akibat serangan ransomware PDN*. Jakarta: Kompas Research Division.

Longstaff, G. (2024). The importance of data privacy law in the digital age. *Law.Ac.UK Blog*.

Marzuki, P. M. (2005). *Penelitian hukum*. Jakarta: Kencana Prenada Media Group.

Muladi, & Arief, B. N. (1992). *Teori-teori dan kebijakan pidana*. Bandung: Alumni.

Muladi. (2002). *Pertanggungjawaban Pidana Korporasi*. Bandung: Refika Aditama.

Muryani, R., & Wiraguna, I. (2024). *Efektivitas UU Perlindungan Data Pribadi dalam Konteks Kelembagaan Pemerintah*. Jurnal Legislasi Indonesia, 21(3), 201–224.

Muryani, R., & Wiraguna, Y. (2024). *Ketimpangan penegakan hukum dalam kasus kebocoran data oleh pemerintah: Analisis hukum pidana*. *Jurnal Hukum & Teknologi*, 9(1), 112–130.

Privacy International. (2025). *Privacy: a fundamental human right*. London: Privacy International.

Rahardjo, S. (2006). *Hukum progresif: Hukum yang membebaskan*. Jakarta: Kompas.

Reddit User Reports. (2024). *Diskusi komunitas seputar kebocoran data PDN dan keamanan sistem digital*. Diakses pada forum komunitas Reddit Indonesia – Cybersecurity Thread (tanpa link).

Soekanto, S., & Mamudji, S. (2001). *Penelitian hukum normatif: Suatu tinjauan singkat*. Jakarta: RajaGrafindo Persada.

Solove, D. J. (2008). *Understanding Privacy*. Harvard University Press.

Sorisa, M. A., Kiareni, S., & Parhusip, A. S. (2024). *Analisis Forensik Digital terhadap Kasus Kebocoran Data BPJS Kesehatan*. Jurnal Kriminologi Digital, 3(1), 45–67.

Tech For Good Institute. (2024). *Cybersecurity Readiness Index: Southeast Asia 2024*. Singapore: TFGI Press.

Teguh, H. (2023). *Kekosongan hukum pidana dalam perlindungan data pribadi oleh lembaga pemerintah*. *Jurnal Graha Kirana*, 5(2), 88–104.

Teguh, R. (2023). Kekosongan hukum pidana dalam perlindungan data pribadi oleh lembaga pemerintah. *Jurnal Hukum dan HAM*, 10(3), 145–162.

Tempo. (2024a). *Ransomware Brain Cipher dan kelumpuhan sistem PDN*. Jakarta: Majalah Tempo, Edisi 2 Juli 2024.

Tempo. (2024b). *Kegagalan pemulihan data PDN dan minimnya sistem backup nasional*. Jakarta: Tempo Investigasi Nasional.

Tommy, F., & Nasution, R. H. (2025). *Konsolidasi data dan problem etika digital dalam administrasi publik Indonesia. Jurnal Administrasi Digital & Teknologi Informasi*, 4(1), 1–18.

Toronto Declaration. (2018). *Protecting the rights to equality and non-discrimination in machine learning systems*. Amnesty International & Access Now.

UN Human Rights Council. (2018). *Report on the right to privacy in the digital age*. New York: United Nations.

UNHRC. (2018). *The right to privacy in the digital age*. Human Rights Council Report A/HRC/39/29.

UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi.

World Jurisprudence. (2025). *International law and digital privacy: Balancing rights and security*. Geneva: WJ Press.

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. New York: PublicAffairs.