JURNAL E-DINAMIC LAW
FAKULTAS HUKUM
UNIVERSITAS BONDOWOSO
Volome 03 Nomor 01 Juli 2024
Website: ejournal.unibo.ac.id
Alamat: Jl. Diponegoro No.247, Selatan Sawah, Kotakulon, kecamatan Kota, Kabupaten Bondowoso, Jawa Timur 68219

PERTANGGUNGJAWABAN HUKUM LEMBAGA NEGARA TERHADAP KEBOCORAN DATA

Achmad Abrari[1], Pramudiarto[2]

[1]*Fakultas Hukum, Universitas Bondowoso*
cak.abrori@gmail.com
[2] *Fakultas Hukum, Universitas Bondowoso*
pramudiarto@gmail.com

Abstract

This study discusses the legal accountability of state institutions regarding personal data breaches in the digital era. Digital transformation has helped the administrative efficiency of state institutions. However, the frequent incidents of data leaks by government institutions, such as the BPJS Kesehatan case, represent a national crisis. Using a normative juridical method, this study finds that Law Number 27 of 2022 on Personal Data Protection regulates the obligations of state institutions to safeguard data security. Although the 1945 Constitution does not explicitly regulate personal data protection, Article 28G paragraph (1) guarantees the right to privacy. The implementation of data protection principles and legal regulations is essential to prevent similar violations and to uphold rights and data security.

Keywords: *Personal Data, Data Leaks, Atate Institution, Legal Accountability*

I. Pendahuluan

Di era digital yang terus berkembang pesat, teknologi informasi telah menjadi elemen kunci dalam berbagai aspek kehidupan, termasuk di sektor pemerintahan. Pemerintah Indonesia, melalui berbagai lembaga negara, telah memanfaatkan kecanggihan teknologi untuk meningkatkan efisiensi pelayanan publik, mempercepat proses administrasi, dan memperluas akses informasi bagi masyarakat. Transformasi digital dalam administrasi negara terlihat dari berbagai inisiatif, seperti *e-government*, layanan publik berbasis daring, dan digitalisasi data kependudukan melalui platform-platform pemerintah.

Lembaga negara di Indonesia secara aktif memanfaatkan Teknologi Informasi dan Komunikasi (TIK) untuk meningkatkan efisiensi layanan publik, transparansi, dan akuntabilitas. Dengan inisiatif seperti *e-government*, digitalisasi layanan publik memungkinkan masyarakat untuk mengakses informasi dan melakukan administrasi tanpa harus datang langsung ke kantor pemerintahan. Contoh nyata penggunaan TIK ini adalah layanan e-KTP, SIM online, dan sistem pajak daring yang memudahkan masyarakat dalam mengurus administrasi.

Penggunaan TIK oleh lembaga negara membawa keuntungan besar, terutama dalam hal efisiensi dan keterbukaan informasi. Proses birokrasi yang sebelumnya panjang dan memakan waktu kini dapat dilakukan dengan lebih cepat dan akurat. Di samping itu, integrasi teknologi memungkinkan lembaga negara untuk menyimpan dan mengelola data dalam jumlah besar secara terpusat, sehingga mempermudah koordinasi lintas sektor.

Penggunaan teknologi ini memungkinkan pemerintah untuk mengelola data dalam jumlah besar dengan lebih efektif, namun di sisi lain, membawa tantangan baru, terutama terkait dengan keamanan data pribadi masyarakat. Kebocoran data, baik akibat serangan siber maupun kelalaian pengelolaan data, menjadi ancaman serius yang dapat merusak kepercayaan publik terhadap pemerintah.

Data pribadi memiliki peran yang sangat penting dalam kehidupan modern, terutama karena banyak aktivitas sehari-hari bergantung pada informasi yang disimpan dan diproses secara digital. Data pribadi mencakup informasi sensitif yang dapat digunakan untuk mengidentifikasi seseorang, seperti nama, alamat, nomor identitas, dan informasi keuangan. Data ini sangat penting untuk melindungi hak-hak individu, menjaga privasi, dan mendukung pelayanan publik oleh pemerintah maupun sektor swasta. Sehingga, keamanan dan pengelolaan data menjadi prioritas dalam konteks modernisasi teknologi.

Kebocoran data dapat menimbulkan berbagai risiko serius, termasuk pencurian identitas, penipuan, dan pelanggaran privasi yang dapat berdampak luas pada individu maupun institusi. Ketika data pribadi bocor dan jatuh ke tangan pihak yang tidak bertanggung jawab, informasi tersebut dapat disalahgunakan untuk kegiatan kriminal, seperti peretasan rekening bank, manipulasi informasi, atau bahkan pemerasan. Kasus seperti kebocoran data BPJS Kesehatan di Indonesia menunjukkan betapa rentannya data individu jika tidak dikelola dengan baik.[1] Data kesehatan, alamat, dan informasi keuangan jutaan orang dijual secara ilegal di pasar gelap, yang berdampak pada keamanan pribadi mereka.

Salah satu kasus kebocoran data yang berdampak signifikan di Indonesia adalah peretasan terhadap Kementerian Komunikasi dan Informatika (KOMINFO). Selain itu, kasus kebocoran data BPJS Kesehatan juga menimbulkan kekhawatiran tentang bagaimana data pribadi dikelola oleh lembaga negara, yang pada akhirnya memengaruhi kepercayaan publik terhadap keamanan data yang dikelola pemerintah.[2] Dalam beberapa tahun terakhir, kasus kebocoran data di Indonesia terus meningkat, termasuk peristiwa-peristiwa besar yang melibatkan data pribadi warga negara, seperti kebocoran data e-KTP, data pelanggan telekomunikasi, dan kasus peretasan yang menimpa Kementerian Komunikasi dan Informatika (KOMINFO).

[1] Humas MENPANRB, Kementerian Pendayagunaan Aparatur Negara Dan Reformasi Birokrasi, *Data BPJS Kesehatan Diduga Bocor, Menteri Tjahjo Dukung Kekominfo Usut Tuntas*, diakses dari https://www.menpan.go.id/site/berita-terkini/data-bpjs-kesehatan-diduga-bocor-menteri-tjahjo-dukung-kemkominfo-usut-tuntas, diakses pada 23 Mei 2021.

Sebagai pengelola data yang bersifat sensitif, lembaga negara memiliki tanggung jawab untuk menjaga keamanan dan kerahasiaan data pribadi warga negara. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi memberikan panduan yang jelas terkait kewajiban lembaga negara dalam melindungi data pribadi dari kebocoran atau penyalahgunaan. Ini termasuk penerapan standar keamanan siber yang ketat dan adanya mekanisme pengawasan yang lebih baik untuk mencegah serangan siber.

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) hadir sebagai respons atas meningkatnya kebutuhan akan perlindungan data pribadi di era digital. UU ini mengatur hak-hak warga negara terkait data pribadi mereka serta mewajibkan lembaga negara dan pihak swasta untuk menjaga keamanan data yang mereka kelola. Namun, meskipun regulasi ini sudah ada, persoalan mengenai pertanggungjawaban hukum lembaga negara dalam kasus kebocoran data tetap menjadi topik yang memerlukan kajian lebih lanjut. Sehingga penulis berminat untuk melakukan penelitian dengan judul 'Pertanggungjawaban Hukum Lembaga Negara Terhadap Kebocoran Data'. Berdasarkan latar belakang tersebut, dapat dirumuskan permasalahan berikut:

1. Bagaimana ketentuan hukum yang mengatur tanggungjawab lembaga negara terhadap kebocoran data menurut peraturan perundang-undangan di Indonesia?
2. Bagaimana implementasi prinsip-prinsip perlindungan data pribadi dalam pertanggungjawaban hukum lembaga negara di Indonesia?

[2] BBC NEWS Indonesia, *BPJS Kesehatan: Data Ratusan Juta Peserta Diduga Bocor-'Otomatis yang Dirugikan Masyarakat', kata pakar*, diakses dari https://www.bbc.com/indonesia/indonesia-57196905, diakses pada 21 Mei 2021.

II. Metode Penelitian

Penelitian ini menggunakan pendekatan yuridis normatif, yaitu pendekatan yang berfokus pada kajian pustaka terhadap bahan-bahan hukum sekunder, seperti peraturan perundang-undangan, doktrin, dan asas hukum yang relevan[3]. Dalam rangka memperoleh pemahaman yang menyeluruh, peneliti menerapkan tiga pendekatan utama. Pertama, pendekatan undang-undang (statute approach), yang dilakukan dengan menelaah secara sistematis peraturan perundang-undangan yang berkaitan. Kedua, pendekatan konseptual (conceptual approach), yang digunakan untuk menggali pemahaman teoretis terkait peran relawan, termasuk motivasi kemanusiaan dan sosial yang mendorong keterlibatan mereka[4].

Selain itu, ruang lingkup penelitian hukum normatif ini mencakup kajian terhadap asas-asas hukum, sistematika hukum, tingkat sinkronisasi hukum secara vertikal dan horizontal, serta penafsiran hukum baik yang tersurat maupun tersirat[5]. Penelitian ini bertujuan untuk menarik dan menganalisis asas hukum yang mendasari keberadaan dan tindakan relawan pengawal ambulans, terutama ditinjau dari asas kemanfaatan dalam konteks pelayanan publik.

III. Result and Discussion

a. Ketentuan Hukum Yang Mengatur Tanggungjawab Lembaga Negara Terhadap Kebocoran Data Menurut Peraturan Perundang-undangan di Indonesia

Dalam era digital yang semakin berkembang, pengelolaan data pribadi menjadi salah satu tanggung jawab utama bagi lembaga negara. Data pribadi tidak hanya berisi informasi yang sangat penting bagi individu, tetapi juga dapat menjadi sumber potensi penyalahgunaan jika tidak dijaga dengan baik. Oleh karena itu, diperlukan ketentuan hukum yang jelas untuk mengatur bagaimana data pribadi harus dikelola, disimpan, dan dilindungi oleh lembaga negara. Ketentuan hukum ini penting untuk memastikan bahwa data yang dimiliki oleh lembaga negara tidak jatuh ke tangan yang salah dan digunakan sesuai dengan tujuan yang sah.

Pentingnya aturan yang mengatur tanggung jawab lembaga negara terhadap kebocoran data juga terkait dengan potensi kerugian yang dapat ditimbulkan.

---

[3] Benuf, K., & Azhar, M. (2020). *Metodologi Penelitian Hukum sebagai Instrumen Mengurai Permasalahan Hukum Kontemporer*. *Gema Keadilan*, *7*(1), 20–33. https://doi.org/10.14710/gk.2020.7504

[4] Negara, T. A. S. (2023). *Normative legal research in Indonesia: Its origins and approaches*. *Audito Comparative Law Journal (ACLJ)*, *4*(1), 1–9. https://doi.org/10.22219/ACLJ.V4I1.24855

[5] Benuf, K. (2020). *Metodologi penelitian hukum normatif: kajian asas, sistematika, sinkronisasi, dan penafsiran hukum*. *Jurnal Gema Keadilan*, *7*(1), 20–33. Diakses dari https://ejournal2.undip.ac.id/index.php/gk/article/download/7504/3859?utm_source=

Kebocoran data bisa berdampak pada banyak pihak, baik itu individu yang datanya bocor, maupun pada kredibilitas dan integritas lembaga negara tersebut. Sehingga, ketentuan hukum tidak hanya berfungsi sebagai dasar bagi lembaga negara untuk mengelola data dengan hati-hati, tetapi juga sebagai upaya untuk melindungi hak-hak individu agar data pribadinya tidak disalahgunakan.

Dengan adanya aturan yang tegas mengenai tanggung jawab hukum lembaga negara dalam hal kebocoran data, diharapkan akan ada sistem yang lebih baik dalam mengatasi potensi pelanggaran terhadap data pribadi. Peraturan tersebut mencakup kewajiban lembaga negara untuk menjaga kerahasiaan data, melakukan pemulihan jika terjadi kebocoran, serta memberikan sanksi terhadap pihak yang terbukti lalai. Semua hal ini bertujuan untuk menciptakan rasa aman bagi masyarakat yang mengandalkan lembaga negara dalam mengelola data pribadi mereka.

Di Indonesia, tanggung jawab lembaga negara terhadap kebocoran data diatur melalui beberapa peraturan perundang-undangan yang mengatur perlindungan data pribadi. Sebagai contoh, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) menjadi dasar hukum utama yang mengatur hak-hak individu terkait dengan data pribadi serta kewajiban bagi lembaga negara atau badan hukum lainnya dalam mengelola data pribadi tersebut dengan cara yang aman dan sesuai dengan hukum. UU ini juga mengatur tentang sanksi bagi pihak yang melanggar ketentuan perlindungan data pribadi, baik secara administratif maupun pidana.

Selain itu, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) yang telah beberapa kali mengalami perubahan, juga memiliki kaitan erat dengan perlindungan data pribadi. Undang-undang ini mengatur tentang penggunaan teknologi informasi dan transaksi elektronik, yang tidak hanya mencakup kegiatan transaksi, tetapi juga mengenai penyebaran informasi yang dapat mencakup data pribadi seseorang. Ketentuan ini semakin penting karena banyak data pribadi yang diproses melalui sistem elektronik dan platform digital yang rentan terhadap kebocoran atau penyalahgunaan.

Kebocoran data, khususnya yang melibatkan lembaga negara, memiliki dampak yang cukup serius. Dalam banyak kasus, kebocoran data dapat mengakibatkan hilangnya kepercayaan masyarakat terhadap lembaga negara tersebut. Lembaga negara yang memiliki tanggung jawab terhadap pengelolaan data pribadi harus memastikan bahwa data yang mereka kelola aman, tidak jatuh ke tangan yang salah, dan digunakan hanya untuk tujuan yang sah. Sehingga, penting bagi lembaga

negara untuk memiliki mekanisme perlindungan yang efektif dan menerapkan kebijakan yang sesuai dengan peraturan perundang-undangan yang berlaku.

Penting juga untuk memahami bahwa tanggung jawab lembaga negara terhadap kebocoran data bukan hanya terbatas pada upaya untuk menghindari kebocoran tersebut, tetapi juga mencakup kewajiban untuk segera menanggulangi dan memberikan pemulihan jika kebocoran data terjadi. Dalam hal ini, peraturan perundang-undangan yang ada mengharuskan lembaga negara untuk memberikan transparansi terkait dengan insiden kebocoran data yang terjadi, serta memberikan hak kepada individu yang datanya bocor untuk memperoleh kompensasi atau ganti rugi jika diperlukan.

Dalam konteks ini, mekanisme pengawasan dan penegakan hukum menjadi hal yang sangat penting. Badan-badan yang berwenang, seperti Badan Perlindungan Data Pribadi (BPDP), memiliki tugas untuk memastikan bahwa lembaga negara dan sektor swasta yang mengelola data pribadi mematuhi ketentuan hukum yang ada. BPDP berperan untuk mengawasi implementasi perlindungan data pribadi di Indonesia, serta memberikan sanksi kepada lembaga yang terbukti melanggar ketentuan yang ada dalam UU PDP.

Selanjutnya, peraturan mengenai tanggung jawab lembaga negara terhadap kebocoran data juga harus diimbangi dengan adanya pemahaman yang jelas dari masyarakat terkait hak-hak mereka atas data pribadi. Dalam hal ini, edukasi mengenai hak perlindungan data pribadi menjadi salah satu upaya penting untuk menanggulangi dampak negatif dari kebocoran data. Seiring dengan perkembangan teknologi dan semakin kompleksnya ancaman terhadap data pribadi, regulasi yang ada harus terus diperbaharui dan disesuaikan dengan dinamika perkembangan teknologi informasi dan komunikasi.

Tanggung jawab lembaga negara terhadap kebocoran data di Indonesia diatur oleh berbagai peraturan perundang-undangan yang memiliki hierarki dan saling melengkapi. Sebagai contoh, kasus kebocoran data yang melibatkan Kementerian Komunikasi dan Informatika (Kominfo) baru-baru ini menunjukkan betapa pentingnya perlindungan terhadap data pribadi yang dikelola oleh lembaga negara. Dalam konteks ini, beberapa peraturan yang secara khusus mengatur tanggung jawab lembaga negara terhadap kebocoran data adalah Undang-Undang Dasar Negara Republik Indonesia 1945 (UUD 1945), Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), dan Undang-Undang Nomor 11 Tahun

2008 tentang Informasi dan Transaksi Elektronik (ITE) yang telah diubah dengan Undang-Undang Nomor 19 Tahun 2016.

UUD 1945 sebagai hukum dasar negara tidak secara langsung mengatur tentang perlindungan data pribadi atau kebocoran data, namun ia menjamin hak atas perlindungan privasi dan informasi pribadi. Pasal 28G ayat (1) UUD 1945 mengatur bahwa setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang berada di bawah kekuasaannya, serta berhak merasa aman dari segala ancaman. Hal ini memberikan landasan hukum yang kuat bagi negara untuk menjaga data pribadi agar tidak disalahgunakan atau bocor ke pihak yang tidak berwenang, sebagai bagian dari hak atas privasi yang dijamin oleh konstitusi.

Pasal 28G ayat (1) UUD 1945 dalam konteks perlindungan data pribadi menunjukkan bahwa meskipun UUD 1945 tidak secara eksplisit menyebutkan perlindungan data pribadi, pasal ini memberikan dasar hukum yang sangat penting untuk menjamin hak atas privasi dan keamanan informasi pribadi warga negara Indonesia. Pasal ini menyatakan bahwa setiap orang berhak atas perlindungan terhadap diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang berada di bawah kekuasaannya, serta berhak merasa aman dari segala ancaman. Dalam konteks kebocoran data, hak atas perlindungan diri pribadi tersebut meliputi data pribadi yang dimiliki individu, yang berpotensi untuk disalahgunakan atau bocor.

Hak atas perlindungan diri pribadi dalam Pasal 28G ayat (1) dapat diinterpretasikan sebagai hak atas privasi, yang meliputi perlindungan terhadap informasi yang berkaitan langsung dengan identitas pribadi seseorang, seperti data pribadi, yang kini semakin banyak dikumpulkan oleh berbagai lembaga, baik pemerintah maupun swasta. Dengan kata lain, meskipun UUD 1945 tidak secara tegas mengatur tentang data pribadi, hak atas privasi ini memberi ruang bagi peraturan perundang-undangan yang lebih spesifik untuk mengatur perlindungan terhadap data pribadi sebagai bagian dari hak asasi manusia. Sehingga, jika ada kebocoran data pribadi, hal ini dapat dianggap sebagai pelanggaran terhadap hak konstitusional individu yang dilindungi oleh Pasal 28G UUD 1945.

Sebagai landasan hukum dasar, Pasal 28G ayat (1) juga memberikan kewajiban kepada negara untuk melindungi hak-hak warga negara, termasuk data pribadi, dengan cara yang sejalan dengan perkembangan teknologi informasi yang semakin pesat. Kebocoran data pribadi, baik oleh lembaga negara maupun pihak lain, tidak hanya melanggar hak atas privasi individu, tetapi juga menciptakan

ketidakamanan yang merugikan masyarakat. Oleh karena itu, dengan landasan konstitusional ini, negara memiliki tanggung jawab untuk memastikan bahwa data pribadi yang dikelola oleh lembaga negara dijaga kerahasiaannya dan dilindungi dari potensi kebocoran atau penyalahgunaan.

Lebih lanjut, dengan adanya jaminan hak atas privasi dalam Pasal 28G, negara dapat menyusun dan menerapkan peraturan-peraturan perundang-undangan yang mengatur secara lebih spesifik tentang perlindungan data pribadi. Salah satu upaya tersebut tercermin dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), yang mengatur dengan lebih detail kewajiban lembaga negara dalam mengelola dan melindungi data pribadi warganya. Dengan demikian, meskipun tidak ada ketentuan yang secara langsung membahas kebocoran data dalam UUD 1945, pasal ini menyediakan landasan hukum yang kuat bagi pengembangan peraturan-peraturan lebih lanjut yang dapat menangani isu-isu terkait perlindungan data pribadi dan kebocoran data.

Secara keseluruhan, meskipun UUD 1945 tidak secara eksplisit mengatur masalah kebocoran data, Pasal 28G ayat (1) memberikan dasar yang jelas bahwa setiap individu berhak dilindungi dari ancaman yang dapat merugikan hak-hak pribadinya, termasuk ancaman kebocoran data pribadi. Negara, dalam hal ini lembaga negara, wajib untuk menjaga agar data pribadi yang dimiliki oleh warga negara tidak jatuh ke tangan yang tidak berwenang, karena itu merupakan bagian dari hak atas privasi yang harus dijaga dan dilindungi sesuai dengan konstitusi.

Namun, pengaturan yang lebih rinci mengenai tanggung jawab lembaga negara terhadap kebocoran data pribadi di Indonesia diatur dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). UU ini mengatur dengan tegas kewajiban lembaga negara, lembaga publik, dan badan hukum lain yang mengelola data pribadi untuk melindungi data yang mereka kelola. UU PDP mewajibkan setiap lembaga negara untuk memastikan bahwa data pribadi yang mereka miliki dijaga kerahasiaannya, tidak disalahgunakan, dan tidak bocor ke pihak yang tidak berhak. Dalam hal kebocoran data, UU ini mengatur prosedur pemulihan dan pemberitahuan kepada individu yang datanya bocor, serta sanksi administratif maupun pidana bagi lembaga yang terbukti lalai dalam menjaga data pribadi yang mereka kelola.

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) memberikan pengaturan yang lebih rinci dan komprehensif mengenai tanggung jawab lembaga negara dalam melindungi data pribadi warganya. Sebelum

adanya UU ini, meskipun terdapat beberapa ketentuan hukum yang mengatur perlindungan data pribadi, banyak pihak yang menganggap perlindungan tersebut kurang memadai, terutama terkait dengan kebocoran data yang terjadi pada lembaga negara atau instansi pemerintah lainnya. UU PDP memberikan dasar hukum yang jelas bagi pemerintah dan lembaga negara dalam mengelola dan melindungi data pribadi.

Dalam UU PDP, terdapat ketentuan yang mengatur kewajiban lembaga negara untuk menjaga keamanan data pribadi, memastikan data tersebut tidak jatuh ke pihak yang tidak berwenang, serta mengambil langkah-langkah preventif terhadap kebocoran data. Pasal 45 misalnya, mengatur tentang kewajiban penyelenggara sistem elektronik yang mengelola data pribadi untuk menjaga agar data yang dikelola tidak bocor atau disalahgunakan. Pasal ini memberikan dasar bagi penegakan hukum apabila terjadi kelalaian atau pelanggaran dalam pengelolaan data pribadi, termasuk memberikan sanksi administratif atau pidana kepada pihak yang bersalah. Dalam konteks kebocoran data oleh lembaga negara, UU PDP memberikan kerangka hukum yang memungkinkan masyarakat untuk mendapatkan perlindungan, serta memastikan adanya mekanisme pertanggungjawaban bagi lembaga yang mengalami kebocoran data.

Selain itu, Pasal 46 UU PDP juga mengatur mengenai hak-hak individu yang terdampak kebocoran data, termasuk hak untuk diberitahukan mengenai kebocoran data pribadi mereka. Ini menunjukkan bahwa negara dan lembaga negara bertanggung jawab tidak hanya untuk mencegah kebocoran data, tetapi juga untuk memastikan pemulihan yang adil bagi individu yang datanya bocor. Dengan adanya ketentuan yang lebih terperinci seperti ini, UU PDP berfungsi untuk memperkuat perlindungan data pribadi secara komprehensif dan memperjelas peran dan tanggung jawab lembaga negara terkait kebocoran data yang terjadi di masa depan.

Tanggung jawab pemerintah atas kebocoran data pribadi mencakup aspek hukum yang meliputi pertanggung jawaban administratif, sanksi pidana, serta kewajiban untuk memberikan perlindungan kepada masyarakat yang datanya bocor.[6] Dalam hal kebocoran data yang melibatkan lembaga negara atau instansi pemerintah, pemerintah tidak hanya bertanggung jawab untuk memulihkan data yang bocor,

[6] Nafiatul Munawaroh, 2024, Hukumonline, *Tanggung Jawab Pemerintah atas Kebocoran Data Pribadi*, diakses dari https://www.hukumonline.com/klinik/a/tanggung-jawab-pemerintah-atas-kebocoran-data-pribadi-lt66881c826cc33/ .

tetapi juga harus memberikan ganti rugi atau perlindungan kepada individu yang menjadi korban kebocoran.

Pemerintah, sebagai pengelola data publik yang besar, juga memiliki kewajiban untuk menerapkan kebijakan yang memastikan data pribadi dikelola dengan standar keamanan yang tinggi. Hal ini semakin penting mengingat lembaga negara sering kali mengelola data yang bersifat sensitif, seperti data identitas, data keuangan, dan data kesehatan. Dalam hal terjadi kebocoran, pemerintah harus segera melakukan pemulihan dan menginformasikan masyarakat yang terdampak, sesuai dengan ketentuan yang ada dalam UU PDP, yang mewajibkan pemberitahuan segera setelah adanya kebocoran data. Ketidakmampuan lembaga negara dalam menjaga data pribadi dapat berisiko terhadap kepercayaan publik terhadap institusi pemerintah itu sendiri.

Di sisi lain, jika kebocoran data terjadi akibat kelalaian atau ketidakmampuan pemerintah dalam mengelola sistem elektronik dengan baik, maka pemerintah juga harus siap menerima sanksi sesuai dengan hukum yang berlaku. Sehingga, pemerintah, dalam hal ini lembaga negara yang terlibat dalam pengelolaan data pribadi, harus memastikan sistem perlindungan yang memadai untuk menghindari terjadinya kebocoran data, termasuk menerapkan pengamanan teknologi yang lebih canggih dan standar operasional yang jelas dalam pengelolaan data pribadi.

Hal ini menunjukkan bahwa tidak hanya kewajiban untuk memulihkan data yang bocor, tetapi juga tanggung jawab hukum pemerintah untuk memastikan pencegahan kebocoran data dengan menerapkan sistem yang aman, serta kesiapan untuk menghadapi sanksi hukum apabila terjadi kelalaian dalam mengelola data pribadi. Hal ini menjadikan perlindungan data pribadi sebagai tanggung jawab yang tidak hanya terbatas pada lembaga pemerintah, tetapi juga mencakup kepercayaan masyarakat terhadap kapasitas pemerintah dalam menjaga keamanan data pribadi.

Kemudian, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE), yang telah diubah dengan Undang-Undang Nomor 19 Tahun 2016, juga berperan dalam mengatur perlindungan data pribadi yang dikelola secara elektronik. UU ITE mengatur tentang penyalahgunaan data pribadi dalam ruang lingkup transaksi elektronik. UU ini mencakup tindak pidana yang berkaitan dengan penggunaan data pribadi secara ilegal, termasuk penyebaran data tanpa izin pemiliknya. Lembaga negara yang terlibat dalam pengelolaan data elektronik, seperti Kominfo, harus memastikan bahwa data yang dikelola melalui sistem elektronik

dilindungi dengan baik agar tidak terjadi kebocoran yang dapat merugikan masyarakat.

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE), yang kemudian diubah dengan Undang-Undang Nomor 19 Tahun 2016, merupakan salah satu peraturan yang secara tidak langsung juga mengatur aspek tanggung jawab lembaga negara terhadap kebocoran data pribadi di Indonesia, terutama dalam hal transaksi elektronik dan pengelolaan informasi di dunia maya. UU ITE ini mengatur mengenai berbagai aspek hukum yang terkait dengan penggunaan teknologi informasi dan transaksi elektronik, termasuk perlindungan data pribadi yang disalurkan melalui media elektronik.

Begitupun dalam UU ITE, meskipun tidak secara eksplisit mengatur tentang perlindungan data pribadi secara rinci seperti halnya UU PDP (Undang-Undang Perlindungan Data Pribadi), tetap memberikan dasar hukum yang sangat penting terkait pengelolaan informasi dan transaksi elektronik yang dapat mencakup data pribadi. Misalnya, dalam Pasal 26 UU ITE yang mengatur mengenai informasi elektronik yang berkaitan dengan hak privasi individu. Pasal ini menyatakan bahwa setiap orang atau lembaga yang memproses informasi elektronik wajib mendapatkan izin dari pihak yang bersangkutan apabila informasi tersebut berkaitan dengan data pribadi.

Selain itu, UU ITE memberikan sanksi terhadap pihak yang melanggar hak privasi melalui pemrosesan atau distribusi informasi pribadi tanpa izin yang sah. Pasal 27 mengatur tentang larangan untuk menyebarkan informasi yang melanggar kesusilaan, pencemaran nama baik, dan atau yang dapat menyebabkan kerugian pihak lain, termasuk data pribadi yang disalahgunakan. Pelanggaran terhadap ketentuan ini bisa berujung pada pidana penjara atau denda, yang secara langsung memberikan tanggung jawab hukum kepada lembaga negara atau pihak yang mengelola data pribadi tersebut, jika kebocoran data tersebut terjadi akibat kelalaian atau pelanggaran hukum.

Ketika kebocoran data terjadi dalam konteks sistem elektronik yang dikelola oleh lembaga negara atau instansi pemerintah, UU ITE memberikan dasar untuk pertanggungjawaban hukum. Dalam hal ini, Pasal 27 yang mengatur tentang penyebaran informasi pribadi secara ilegal, serta Pasal 28 yang mengatur tentang penyebaran hoaks atau informasi palsu yang merugikan orang lain, bisa digunakan untuk menuntut lembaga yang bertanggung jawab atas kebocoran data. Selain itu, Pasal 32 dan Pasal 33 UU ITE mengatur mengenai kewajiban penyelenggara sistem

elektronik untuk menjaga kerahasiaan dan integritas data yang ada dalam sistem tersebut. Dalam hal terjadi kebocoran data akibat kelalaian atau kelalaian sistem, lembaga negara bisa dikenakan sanksi sesuai dengan ketentuan hukum yang berlaku.

Salah satu poin penting yang diatur dalam UU ITE, terutama setelah revisinya dengan UU Nomor 19 Tahun 2016, adalah pentingnya pengelolaan sistem elektronik yang aman. Pasal 31 mengatur kewajiban bagi penyelenggara sistem elektronik untuk memenuhi standar keamanan yang memadai, termasuk melakukan perlindungan terhadap data pribadi yang dikelola melalui sistem elektronik. Hal ini menjadi relevan dalam konteks kebocoran data pribadi yang melibatkan lembaga negara, di mana standar keamanan yang tidak memadai dapat menjadi penyebab utama kebocoran tersebut.

UU ITE memberikan sanksi bagi lembaga negara atau penyelenggara sistem elektronik yang terbukti gagal dalam mengelola data pribadi atau informasi elektronik secara aman. Pasal 46 dan Pasal 47 mengatur tentang sanksi pidana bagi mereka yang terbukti dengan sengaja atau karena kelalaiannya menyebabkan kebocoran data pribadi. Di sisi lain, undang-undang ini juga memberikan mekanisme hukum yang jelas untuk mengatasi masalah ini dengan memberikan perlindungan kepada individu yang datanya bocor, termasuk melalui mekanisme ganti rugi atau kompensasi.

Untuk memperkuat pengawasan terhadap implementasi perlindungan data pribadi, Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik juga mengatur kewajiban penyelenggara sistem elektronik, baik itu pemerintah maupun swasta, untuk menjaga data pribadi yang mereka kelola. Peraturan ini memberikan pedoman teknis untuk memastikan bahwa sistem elektronik yang digunakan dapat melindungi data pribadi secara maksimal dari ancaman kebocoran dan serangan siber.

Dengan demikian, meskipun kebocoran data seperti yang terjadi pada Kominfo menjadi permasalahan serius, Indonesia telah memiliki dasar hukum yang cukup lengkap untuk mengatur tanggung jawab lembaga negara dalam hal perlindungan data pribadi. Dari UUD 1945 sebagai dasar konstitusional, hingga UU PDP dan UU ITE yang memberikan pengaturan yang lebih rinci, negara memiliki kewajiban untuk memastikan bahwa data pribadi masyarakat dilindungi dengan baik, dan jika terjadi kebocoran, mekanisme pemulihan serta sanksi yang sesuai dapat diterapkan.

b. Implementasi Prinsip-Prinsip Perlindungan Data Pribadi Dalam Pertanggungjawaban Hukum Lembaga Negara Di Indonesia

Dalam era digital ini, data pribadi telah menjadi salah satu aset paling berharga yang dimiliki oleh individu dan organisasi. Setiap hari, kita menghasilkan, membagikan, dan memproses data pribadi, baik melalui media sosial, transaksi keuangan online, maupun dalam hal-hal administratif lainnya. Namun, perkembangan pesat teknologi informasi dan komunikasi tidak hanya menawarkan kemudahan tetapi juga risiko, termasuk risiko kebocoran data yang dapat merugikan individu maupun organisasi. Data pribadi yang bocor atau disalahgunakan bisa berdampak serius, mulai dari pencurian identitas hingga penyalahgunaan yang merugikan hak-hak individu. Kondisi ini menjadikan perlindungan data pribadi sebagai isu penting di seluruh dunia, termasuk di Indonesia.

Perlindungan data pribadi bukan hanya menjadi perhatian bagi perusahaan atau penyedia layanan digital, tetapi juga bagi lembaga negara. Sebagai pengelola data dari jutaan warga negara, lembaga negara memiliki peran yang sangat strategis dalam menjaga keamanan data pribadi warga negara yang ada di bawah tanggung jawab mereka. Lembaga negara tidak hanya dituntut untuk menjaga data yang mereka kelola, tetapi juga bertanggung jawab secara hukum apabila terjadi kebocoran atau penyalahgunaan data. Dalam konteks ini, penting untuk memahami bagaimana prinsip-prinsip perlindungan data pribadi diimplementasikan dalam sistem hukum Indonesia, khususnya dalam konteks tanggung jawab lembaga negara.

Selain berperan sebagai pelindung, lembaga negara juga memiliki kewajiban hukum yang melekat dalam pengelolaan data pribadi. Kewajiban ini mencakup pengamanan data, pengelolaan data yang akuntabel, serta penerapan sistem yang sesuai dengan standar keamanan yang berlaku. Kewajiban-kewajiban tersebut telah diatur dalam berbagai peraturan perundang-undangan di Indonesia yang menetapkan tanggung jawab lembaga negara dalam melindungi data pribadi, terutama mengingat kasus-kasus kebocoran data yang baru-baru ini terjadi di beberapa instansi pemerintah. Peristiwa-peristiwa ini menambah urgensi perlunya implementasi hukum yang kuat dalam melindungi data pribadi.

Tanggung jawab lembaga negara dalam perlindungan data pribadi tidak hanya sebatas kewajiban administratif, melainkan juga merupakan wujud dari prinsip-prinsip keadilan yang harus dijalankan oleh pemerintah kepada warganya. Dalam hal ini, negara tidak hanya berfungsi sebagai pengatur, tetapi juga sebagai penjamin bahwa data pribadi yang dikelola oleh instansi negara akan terlindungi

dengan baik dan tidak disalahgunakan. Konsep ini sejalan dengan prinsip perlindungan hak asasi manusia yang menjamin privasi individu sebagai bagian dari hak-hak dasar yang harus dijamin oleh negara.

Dengan memahami prinsip-prinsip dasar perlindungan data pribadi, kita dapat mengevaluasi bagaimana implementasinya dalam pertanggungjawaban hukum lembaga negara di Indonesia. Prinsip-prinsip ini, yang mencakup aspek keamanan, transparansi, dan tanggung jawab, akan menjadi fokus utama dalam pembahasan selanjutnya. Menelaah penerapan prinsip-prinsip ini dalam konteks hukum di Indonesia memberikan gambaran tentang sejauh mana perlindungan data pribadi telah dijamin oleh lembaga negara dan apa yang perlu diperkuat untuk mencegah kebocoran data di masa depan.

Implementasi prinsip-prinsip perlindungan data pribadi dalam pertanggungjawaban hukum lembaga negara di Indonesia menjadi sangat penting, terutama dalam menjaga kepercayaan masyarakat terhadap sistem pemerintahan. Salah satu ahli hukum yang memberikan penjelasan mendalam tentang prinsip-prinsip perlindungan data pribadi adalah Sudikno Mertokusumo. Menurut Mertokusumo, perlindungan data pribadi dalam konteks hukum tidak dapat dilepaskan dari prinsip-prinsip dasar yang mencakup aspek keamanan, kerahasiaan, akuntabilitas, dan kepatuhan terhadap peraturan.[7] Prinsip-prinsip ini tidak hanya sekedar norma administratif, tetapi merupakan bagian dari hak asasi manusia yang dijamin oleh konstitusi dan berbagai peraturan terkait. Dalam konteks hukum Indonesia, upaya untuk menerapkan prinsip-prinsip ini secara tegas masih menghadapi berbagai tantangan, terutama terkait infrastruktur hukum dan teknologi.

Salah satu prinsip utama dalam perlindungan data pribadi adalah keamanan. Prinsip ini menekankan pentingnya menjaga data dari akses yang tidak sah atau penyalahgunaan, sehingga setiap penyelenggara data pribadi harus menerapkan langkah-langkah keamanan yang efektif. Keamanan data menjadi tanggung jawab lembaga negara agar data warga negara tidak mudah diakses atau dicuri oleh pihak yang tidak berwenang. UU Perlindungan Data Pribadi (UU PDP) yang baru disahkan di Indonesia telah memberikan dasar hukum yang lebih jelas bagi lembaga negara dalam menjaga keamanan data pribadi. UU ini menetapkan bahwa setiap penyelenggara data pribadi wajib menerapkan sistem keamanan yang memadai untuk mencegah risiko kebocoran atau penyalahgunaan data. Namun, pelaksanaan

[7] Sudikno Mertokusumo, 2021, *Teori Hukum: Suatu Pengantar*, (Jakarta: Universitas Atma Jaya), p.213

keamanan data ini memerlukan infrastruktur teknologi dan manajemen data yang kuat, yang terkadang menjadi tantangan di banyak lembaga negara di Indonesia.

Selain keamanan, prinsip kerahasiaan menjadi unsur penting dalam implementasi perlindungan data pribadi. Prinsip kerahasiaan mengharuskan data pribadi yang dikumpulkan tidak diungkapkan tanpa persetujuan pemilik data, kecuali jika diatur sebaliknya oleh hukum. Lembaga negara memiliki kewajiban untuk menjaga kerahasiaan data pribadi yang mereka kelola, baik dalam pengumpulan, penyimpanan, maupun pemrosesan data tersebut. Kerahasiaan ini termasuk kewajiban untuk tidak memberikan data kepada pihak ketiga tanpa persetujuan dari pemilik data, kecuali dalam keadaan yang telah diatur secara khusus oleh undang-undang. UU ITE dan UU PDP telah memperkuat dasar hukum dalam menjaga kerahasiaan data pribadi, namun masih terdapat beberapa kasus yang menunjukkan adanya kebocoran data yang diduga disebabkan oleh kelalaian dalam menjaga kerahasiaan tersebut.

Prinsip akuntabilitas juga merupakan bagian penting dari tanggung jawab lembaga negara terhadap perlindungan data pribadi. Mertokusumo menegaskan bahwa prinsip akuntabilitas mewajibkan penyelenggara data untuk bertanggung jawab atas setiap pengelolaan data yang dilakukan, termasuk tindakan yang perlu diambil dalam kasus kebocoran data. Akuntabilitas di sini berarti bahwa lembaga negara harus siap mempertanggungjawabkan setiap tindakan yang dilakukan terkait data pribadi yang mereka kelola. Jika terjadi kebocoran data, lembaga terkait harus menjelaskan kepada publik atau pemilik data tentang penyebab insiden tersebut serta langkah-langkah perbaikan yang akan diambil. Penerapan akuntabilitas ini menciptakan transparansi dan membangun kepercayaan publik terhadap lembaga negara dalam mengelola data pribadi.

Kepatuhan terhadap peraturan menjadi prinsip lain yang tak kalah penting dalam melaksanakan tanggung jawab hukum terhadap perlindungan data pribadi. Prinsip kepatuhan terhadap peraturan mencerminkan kewajiban untuk menjalankan pengelolaan data sesuai dengan peraturan yang berlaku dan standar yang telah ditetapkan. Setiap lembaga negara harus mematuhi standar perlindungan data yang ditetapkan oleh undang-undang dan peraturan pemerintah. UU PDP, UU ITE, dan berbagai regulasi turunan lainnya memberikan standar operasional yang jelas mengenai perlindungan data pribadi. Namun, kepatuhan ini memerlukan pengawasan dan penegakan hukum yang konsisten. Pengawasan yang efektif akan memastikan

bahwa lembaga negara tidak hanya mengikuti prosedur yang ditetapkan, tetapi juga mematuhi prinsip-prinsip perlindungan data dalam operasional sehari-hari.

Implementasi prinsip-prinsip ini juga memerlukan peningkatan kapasitas teknologi dan sumber daya manusia. Banyak lembaga negara yang masih menghadapi keterbatasan dalam infrastruktur teknologi yang memadai untuk pengelolaan data yang aman dan handal. Di samping itu, pelatihan bagi sumber daya manusia di lingkungan pemerintahan untuk memahami pentingnya perlindungan data pribadi juga menjadi faktor kunci. Tanpa dukungan teknologi yang baik dan personel yang terlatih, upaya penerapan prinsip-prinsip perlindungan data pribadi akan sulit mencapai hasil yang optimal.

Seiring dengan meningkatnya kesadaran akan pentingnya perlindungan data pribadi, pemerintah telah memperkuat regulasi untuk menanggapi masalah kebocoran data di lembaga negara. Namun, tantangan dalam implementasi tetap ada, khususnya terkait dengan konsistensi penegakan hukum dan evaluasi terhadap standar keamanan yang ada. Pengawasan dan evaluasi yang berkelanjutan akan memastikan bahwa prinsip-prinsip perlindungan data pribadi benar-benar diterapkan oleh lembaga negara, serta menjadi bagian dari tanggung jawab hukum yang wajib mereka jalankan.

Dalam kasus kebocoran data Bjorka, yang menyeret Kementerian Komunikasi dan Informatika (KOMINFO) ke perhatian publik, penerapan prinsip-prinsip perlindungan data pribadi menjadi sangat relevan. Kebocoran ini mengungkap tantangan besar dalam pengamanan data di instansi pemerintah. Menurut UU Perlindungan Data Pribadi, tanggung jawab hukum KOMINFO mencakup perlindungan keamanan data serta akuntabilitas dalam setiap aspek pengelolaannya. Tanggung jawab ini mencakup kewajiban KOMINFO untuk menanggulangi kebocoran dengan mengidentifikasi celah keamanan serta mengambil tindakan pemulihan terhadap kerugian yang diderita masyarakat.

Prinsip akuntabilitas yang tercantum dalam UU PDP menuntut lembaga negara untuk transparan dalam penanganan data pribadi. Dalam kasus Bjorka, KOMINFO menerima kritik karena dianggap kurang terbuka dalam menginformasikan penyebab kebocoran dan langkah perbaikan yang diambil. Transparansi ini sangat penting untuk membangun kembali kepercayaan masyarakat, terutama karena data pribadi adalah bagian dari hak privasi warga negara yang

dilindungi oleh hukum.[8] UU PDP juga menyatakan bahwa lembaga penyelenggara data harus melaporkan setiap insiden kebocoran secara terbuka untuk mencegah penyalahgunaan lebih lanjut.

Sikap proaktif dalam memperbaiki sistem keamanan menjadi langkah penting yang diharapkan masyarakat dari KOMINFO. Berdasarkan analisis dari artikel ITS News, kebocoran data menunjukkan bahwa pemerintah perlu meningkatkan teknologi enkripsi dan memutakhirkan sistem keamanannya secara berkala untuk melawan ancaman peretasan. Langkah ini juga melibatkan pengembangan prosedur keamanan yang lebih ketat dan pelatihan personel di lembaga negara agar mampu menjaga data dengan lebih efektif.

Sebagai lembaga yang bertanggung jawab dalam bidang komunikasi dan informasi, KOMINFO memiliki peran penting dalam mensosialisasikan pentingnya perlindungan data. Sikap preventif dengan memberikan edukasi terkait keamanan data kepada masyarakat dapat membantu meningkatkan kesadaran tentang risiko-risiko kebocoran data dan cara melindungi data pribadi. Hal ini selaras dengan prinsip kepatuhan terhadap peraturan yang diamanatkan oleh UU PDP, yang juga mewajibkan lembaga pemerintah untuk memastikan setiap prosedur pengelolaan data sesuai dengan ketentuan yang berlaku.

Di samping itu, KOMINFO diharapkan menjalin kerja sama dengan lembaga lain yang berfokus pada keamanan siber. Kolaborasi ini penting untuk merespons serangan data dengan cepat dan efektif. Sebagai contoh, kerja sama dengan Badan Siber dan Sandi Negara (BSSN) dapat membantu dalam pemantauan sistem keamanan dan respons cepat terhadap insiden keamanan data. Dengan memperkuat koordinasi antarlembaga, upaya mitigasi kebocoran data bisa dilakukan lebih efektif dan efisien.

Perlindungan data membutuhkan sinergi antara pemerintah, penyedia layanan digital, dan pengguna. Implementasi regulasi yang lebih ketat, termasuk edukasi kepada masyarakat tentang keamanan data, sangat dibutuhkan. Kasus kebocoran data seperti yang dilakukan oleh Bjorka menjadi peringatan tentang kelemahan sistem yang ada dan mendorong urgensi penguatan sistem keamanan digital di Indonesia.

Dengan adanya UU PDP, KOMINFO memiliki kewajiban yang jelas untuk tidak hanya mengamankan data pribadi, tetapi juga bertindak proaktif dalam hal kebocoran data. Implementasi prinsip-prinsip perlindungan data seperti keamanan,

[8] Itsojt, ITS News, (2022, November 2), *Menyikapi Kasus Kebocoran Data Pribadi di Era Digital*, diakses dari: https://www.its.ac.id/news/2022/11/02/menyikapi-kasus-kebocoran-data-pribadi-di-era-digital/

kerahasiaan, akuntabilitas, dan kepatuhan dalam lingkup kerja KOMINFO mencerminkan komitmen untuk menjaga hak-hak privasi masyarakat dan memperkuat kepercayaan publik terhadap lembaga negara.

IV. Conclusion and Suggestion

Berdasarkan pembahasan tentang tanggung jawab hukum lembaga negara terhadap kebocoran data, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) memberikan landasan yang jelas. Meskipun UUD 1945 tidak secara langsung mengatur perlindungan data pribadi, Pasal 28G ayat (1) menjamin hak atas privasi. UU PDP, khususnya Pasal 45, mengharuskan lembaga negara, termasuk KOMINFO, untuk bertanggung jawab atas kebocoran data, memastikan keamanan, serta melakukan pemulihan dan pemberian ganti rugi jika terjadi pelanggaran terhadap hak-hak individu terkait data pribadi.

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) menetapkan prinsip akuntabilitas, keamanan, dan transparansi dalam pengelolaan data oleh lembaga negara, termasuk KOMINFO. UU ini mewajibkan pelaporan terbuka atas insiden kebocoran dan pemulihan data sebagai bentuk akuntabilitas. Lembaga negara juga diharapkan mengimplementasikan sistem perlindungan data yang kuat guna mencegah insiden serupa dan membangun kembali kepercayaan publik terhadap upaya pemerintah dalam menjaga data pribadi sesuai peraturan yang berlaku.

Referensi

Buku

Asikin, Muhammad. 2019. *Hukum Privasi dan Perlindungan Data Pribadi.* (Jakarta: Sinar Grafika).

Hartono, Sunaryati. 2018. *Asas-Asas Tanggung jawab Hukum.* (Bandung: Alumni).

Marzuki, Peter Mahmud. 2020. *Pengantar Ilmu Hukum.* (Jakarta : Kencana).

Mertokusumo, Sudikno. 2020. *Pengantar Ilmu Hukum.* (Yogyakarta: Liberty).

Mertokusumo. 2021. *Teori Hukum: Suatu Pengantar.* (Jakarta: Universitas Atma Jaya).

Rahardjo, Satjipto. 2018. *Hukum dan Perubahan Sosial.* (Yogyakarta: Genta Publishing).

Raharjo, Satjipto. 2020. *Prinsip-Prinsip Hukum Perlindungan Data Pribadi.* (Yogyakarta: UGM Press).

Schubert, Winfried H. 2016. *Hukum Perlindungan Data Pribadi.* (Jakarta: Raja Grafindo Persada).

Soekanto, Soerjono. 2019. *Pengantar Penelitian Hukum.* (Jakarta: UI Press).

Soerjono, Soekanto. 2012. *Perlindungan Hukum bagi Warga Negara Indonesia.* (Jakarta: Raja Grafindo Persada).

Solove, Daniel J. 2011. *Pemahaman tentang Privasi.* (Jakarta: Pustaka Pelajar).

Subekti, R. 2014. *Perlindungan Hukum Terhadap Hak dalam Sistem Hukum Indonesia.* (Jakarta: IKAPI).

Suteki, Moh. 2020. *Hukum Perlindungan Data Pribadi di Indonesia.* (Bandung: PT Refika Aditama).

Syahab, H. 2021. *Perlindungan Data Pribadi dalam Sistem Hukum Indonesia.* (Jakarta: Kencana).

Website

BBC NEWS Indonesia. 2021. *BPJS Kesehatan: Data Ratusan Juta Peserta Diduga Bocor-'Otomatis yang Dirugikan Masyarakat', kata pakar*. BBC NEWS. Diakses pada: https://www.bbc.com/indonesia/indonesia-57196905

Hakim, Lukman Nur. 2024. *Tak Ada Indonesia, Ini 8 Negara dengan Kasus Kebocoran Data Terbanyak di Dunia.* Jakarta: Bisnis.com. Diakses pada: https://teknologi.bisnis.com/read/20241028/84/1811093/tak-ada-indonesia-ini-8-negara-dengan-kasus-kebocoran-data-terbanyak-di-dunia

Humas MENPANRB. 2021. *Data BPJS Kesehatan Diduga Bocor, Menteri Tjahjo Dukung Kekominfo Usut Tuntas*. Jakarta: PARNB Kementerian Pendayagunaan Aparatur Negara Dan Reformasi Birokrasi. Diakses pada: https://www.menpan.go.id/site/berita-terkini/data-bpjs-kesehatan-diduga-bocor-menteri-tjahjo-dukung-kemkominfo-usut-tuntas

Itsojt. 2022. *Menyikapi Kasus Kebocoran Data Pribadi di Era Digital.* Surabaya: ITS News. Diakses pada: *Menyikapi Kasus Kebocoran Data Pribadi di Era Digital*, https://www.its.ac.id/news/2022/11/02/menyikapi-kasus-kebocoran-data-pribadi-di-era-digital/

Munawaroh, Nafiatul. 2024. *Tanggung Jawab Pemerintah atas Kebocoran Data Pribadi.* Jakarta: Hukum Online. Diakses pada: https://www.hukumonline.com/klinik/a/tanggung-jawab-pemerintah-atas-kebocoran-data-pribadi-lt66881c826cc33/

Sloan, MIT. 2024. *MIT report details new cybersecurity risks.* Cambridge: MIT Management Sloan School. Diakses pada: https://mitsloan.mit.edu/

Sumber Hukum

Undang-Undang Dasar Negara Republik Indonesia 1945 (UUD 1945).

Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE).

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP).