

PERLINDUNGAN DATA PRIBADI WARGA NEGARA INDONESIA TERKAIT DENGAN KEBOCORAN DATA

Hezkiel Bram Setiawan¹ & Fatma Ulfatun Najicha²

Informatika, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Sebelas Maret¹

Ilmu Hukum, Fakultas Hukum, Universitas Sebelas Maret²

Email : hezkielbramsetiawan@student.uns.ac.id¹ & fatmanajicha_law@staff.uns.ac.id²

Abstrak

Perkembangan digital dan keterbukaan terhadap transaksi online seringkali berujung pada kebocoran data. Di satu sisi, perkembangan digital memberikan manfaat bagi ekonomi digital, tetapi di saat yang sama juga dapat menimbulkan dampak atau ancaman baru bagi ekonomi konvensional dari aspek kerentanan keamanan siber hingga merugikan informasi pelanggan dan menantang konsep privasi. Kurangnya persetujuan pemerintah pada perlindungan data terhadap UUD 1945 adalah salah satu contoh penyebabnya. Penelitian ini bertujuan untuk mengusulkan dipercepatnya pengesahan RUU Perlindungan Data Pribadi Indonesia oleh Dewan Perwakilan Rakyat (DPR). Metode penelitian yang dipakai untuk penelitian ini adalah metode yuridis normatif dengan menggunakan pendekatan undang-undang. Data yang digunakan untuk penelitian ini adalah data sekunder yang berdasar atas bahan hukum primer dan hukum sekunder. Hasil penelitian menunjukkan urgensi untuk merancang peraturan baru sebelum menangani masalah kebocoran data dan menjaga kerahasiaan data pribadi warga negara Indonesia. Melalui UU PDP yang berlaku akan menguntungkan para pemangku kepentingan, pemilik data, dan pengakuan lebih lanjut oleh negara lain.

Kata kunci: Perlindungan Data Pribadi, Rancangan Undang-Undang, Kebocoran Data

Abstract

Digital developments and openness to online transactions often lead to data leaks. Digital developments provide advantages for the digital economy, but on the other hand it can also create new impacts or threats to the conventional economy, from cybersecurity vulnerabilities to harming customer information and challenging the concept of privacy. The lack of government approval on data protection of the 1945 Constitution is one example of the cause. This study aims to propose an accelerated ratification of the Indonesian Personal Data Protection Bill by the House of Representatives. The research method used for this research is a normative juridical method with a law approach. The data used for this research is secondary data based on primary and secondary legal materials. The results of the study indicate the urgency to draft new regulations before dealing with the problem of data leakage and maintaining the confidentiality of the personal data of Indonesian citizens. Through the applicable PDP Law, it will benefit stakeholders, data owners, and further recognition by other countries.

Keywords: Personal Data Protection, Draft Bill, Data Leak



Ciptaan disebarluaskan di bawah [Lisensi Creative Commons Atribusi-BerbagiSerupa 4.0 Internasional](https://creativecommons.org/licenses/by-sa/4.0/).

PENDAHULUAN

Data yang dirilis oleh APJII tentang penetrasi pemakai internet yang berada di wilayah Indonesia pada periode tahun 2019 hingga tahun 2020 menunjukkan adanya peningkatan jumlah pengguna internet mengakibatkan peningkatan kasus kebocoran data di Indonesia. Disebutkan

penetrasi pengguna internet mencapai sekitar seratus sembilan puluh juta orang dari total penduduk Indonesia sekitar dua ratus enam puluh enam juta orang (Tim Survei APJII, 2021). Artinya, kemajuan teknologi telah menyentuh sekitar 73,7% warga Indonesia. Kemajuan teknologi ini juga membawa keamanan siber, ancaman,

dan masalah perlindungan data, yang dapat berdampak pada keselamatan publik. Hal ini akhirnya mengarah pada adopsi perjanjian internasional pertama yang menangani kejahatan komputer dan internet, yaitu Konvensi Dewan Eropa tentang Kejahatan Dunia Maya, yang diadopsi pada tahun 2001. Adopsi perjanjian ini memiliki tiga tujuan, yaitu menyelaraskan hukum kejahatan dunia maya substantif lintas batas, menyelaraskan aturan prosedur yang relevan dengan investigasi kriminal dengan komponen digital, dan menerapkan kerangka kerjasama penegakan hukum internasional yang praktis dalam kasus-kasus kejahatan dunia maya (Council of Europe, 2001).

Kemudian, berdasarkan penelitian Hootsuite, ditemukan bahwa lebih dari setengah populasi, yaitu 64% dari populasi Indonesia, terhubung ke internet (Hootsuite, 2020). Data warga Indonesia tersebut seringkali bisa diakses oleh pihak ilegal karena memiliki potensi kebocoran data yang besar. Data milik Yayasan Lembaga Konsumen Indonesia (YLKI) mengenai pencurian data pribadi pada tahun 2019 mencatat pencurian data paling banyak dilakukan pada sektor perbankan, yaitu dengan kasus sebanyak 106, disusul pinjaman online dengan kasus sebanyak 96, perumahan dengan kasus sebanyak 81, belanja online dengan kasus sebanyak 34, dan leasing dengan kasus sebanyak 32. Pengaduan kasus juga meningkat drastis pada masa pandemi karena penggunaan perdagangan elektronik atau e-commerce sebagai platform belanja meningkat. Ketika pembatasan aktivitas dilakukan pada masa pandemi, data menunjukkan ada 54 kasus pencurian data perdagangan elektronik dari 277 kasus dari Januari 2020 hingga Juni 2020 (Hidayah, A. A., & Ezerli, S., 2020).

Privasi, secara umum, dapat didefinisikan dengan berbagai arti. Menurut Kamus Cambridge, privasi didefinisikan sebagai hak untuk merahasiakan kehidupan pribadi atau informasi pribadi mereka. Menurut Warren and Brandeis, privasi adalah aturan untuk menikmati hidup dan hak untuk dibiarkan sendiri. Perkembangan Hukum ini tidak dapat dihindari dan menuntut pengakuan hukum (Warren and Brandeis, 1890).

Pada tanggal 31 Mei 2021, Indonesia dihebohkan dengan berita bocornya data pribadi 279 juta orang Indonesia dan dijual di situs Raidforums seharga 0,15 Bitcoin (70-80 juta rupiah). Kemudian sama halnya dengan kasus lain yang menimpa Tokopedia, yang pada dasarnya merugikan konsumen. Diperkirakan jumlahnya mencapai 91 juta akun user dan 7 juta akun merchant mengalami kebocoran data. Akun-akun tersebut dijual dengan harga 5000 dolar Amerika atau sekitar 74 juta rupiah di situs Raidforums juga (Assifa, F., 2021). Kasus-kasus tersebut hanyalah sebagian kecil contoh kebocoran data yang diunggah di situs Raidforums. Hal ini sangat merugikan ekonomi digital Indonesia terutama dalam masa pandemi. Tindakan yang dilakukan oleh Kementerian Komunikasi dan Informatika adalah menutup akses untuk mengunduh data serta memblokir situs ini.

Dalam praktik melindungi data pribadi, khususnya terhadap konsumen yang aktif di internet atau pengguna platform digital, hak privasinya dilindungi oleh Undang-Undang Dasar 1945 (UUD 1945) yang diturunkan amanatnya ke dalam beberapa peraturan, yaitu Undang-Undang Nomor 23 Tahun 2006 sebagaimana telah diubah dengan Undang-Undang Nomor 24 Tahun 2013 tentang Administrasi Kependudukan Republik Indonesia (AKRI), Undang-Undang Nomor 11 Tahun 2008 sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun

2016 tentang Informasi dan Transaksi Elektronik (ITE), Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP IEST), Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik. Sementara itu, dalam lingkup global, perlindungan data pribadi diatur melalui beberapa ketentuan, antara lain Deklarasi Hak Asasi Manusia (UDHR), General Data Protection Regulation (GDPR) Uni Eropa, International Convention on Civil and Political Rights (ICCPR).

Namun, undang-undang yang ada saat ini dinilai masih belum komprehensif dan tegas dalam menyelesaikan permasalahan terkait perlindungan data pribadi di Indonesia. Oleh karena itu, pada tahun 2018 melalui Kementerian Penerangan, diciptakanlah RUU baru tentang Undang-Undang Perlindungan Data Pribadi.

METODE PENELITIAN

Penelitian ini menggunakan metode yuridis normatif dengan pendekatan undang-undang. Data yang digunakan adalah data sekunder yang terdiri dari sumber hukum primer dan sekunder. Sumber hukum primer terdiri dari UUD 1945, Undang-Undang Nomor 23 Tahun 2006 sebagaimana telah diubah dengan Undang-Undang Nomor 24 Tahun 2013 tentang Administrasi Kependudukan Republik Indonesia (AKRI), Undang-Undang Nomor 11 Tahun 2008 sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (ITE), Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP IEST), Peraturan Menteri Komunikasi dan Informatika Nomor 20

Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik.

Bahan hukum sekunder menggunakan jurnal ilmiah, buku, dan dokumen hukum terkait lainnya. Data penelitian yang digunakan adalah penelitian kepustakaan, yang berarti penulis membaca, memahami, dan akhirnya menulis kesimpulan dari peraturan perundang-undangan, buku, jurnal, berita, dan artikel yang berkaitan dengan topik. Metode analisis data menggunakan yuridis kualitatif yang membandingkan data yang diperoleh dengan aturan hukum, konvensi, dan peraturan terkait lainnya untuk menafsirkan masalah.

HASIL PENELITIAN DAN PEMBAHASAN

Hasil Penelitian

Berdasarkan hasil penelitian dari berbagai macam sumber, ditemukan keurgensian untuk merancang peraturan baru mengenai data pribadi warga negara Indonesia serta menangani masalah kebocoran data dan menjaga kerahasiaan data pribadi warga negara Indonesia.

Kepastian hukum merupakan salah satu esensi kehidupan berbangsa dan bernegara yang patut dijunjung tinggi oleh seluruh warga Indonesia, termasuk pada dunia maya sekalipun. Dengan adanya Rancangan Undang-Undang Perlindungan Data Pribadi, warga Indonesia akan mendapat kepastian hukum. Rancangan Undang-Undang juga dapat mengurangi kemungkinan pengaksesan data pribadi warga Indonesia oleh oknum tanpa izin.

Rancangan Undang-Undang Perlindungan Data Pribadi diharapkan dapat menjaga kerahasiaan data pribadi warga negara Indonesia. RUU ini juga bisa menjadi solusi untuk warga Indonesia dalam pengelolaan data pribadi.

Kasus-kasus kebocoran data pribadi yang muncul adalah suatu contoh dari kurangnya kepastian hukum terhadap

warga Indonesia. Data pribadi yang ada bisa mudah diakses oleh oknum yang tidak bertanggung jawab. Oknum yang melakukan tindak kejahatan ini juga tidak dihukum dengan seadilnya karena kepastian hukum yang kurang. Bahkan, oknum bisa kabur tanpa meninggalkan jejak apapun.

Pembahasan

Perkembangan teknologi komunikasi informasi berbasis komputer telah berkembang di masyarakat, yaitu segala sesuatu yang berhubungan dengan akses internet. Di satu sisi, keberadaan internet di masyarakat tentu membuat segala sesuatunya menjadi lebih mudah, praktis, dan efisien. Namun, di sisi lain juga menimbulkan sejumlah permasalahan, termasuk di bidang hukum, salah satunya berkaitan dengan perlindungan data pribadi. Interaksi publik yang menggunakan teknologi informasi sangat bergantung pada ketersediaan, integritas, dan kerahasiaan informasi di ruang siber.

Contohnya pada penggunaan media sosial sebagai sarana komunikasi lintas negara. Teknologi informasi dapat digunakan sebagai media yang efektif untuk mempengaruhi masyarakat dengan menginformasikan opini positif. Meskipun di sisi lain, teknologi informasi juga menjadi ancaman bagi bangsa dan negara jika digunakan untuk menyebarkan konten negatif, bahkan untuk tujuan yang merusak. Apalagi teknologi informasi saat ini menjadi "pedang bermata dua". Berbagai upaya perlindungan data pengguna dipisahkan melalui beberapa perangkat hukum yang disebutkan dalam undang-undang yang berbeda, sebagaimana tertuang dalam Peraturan Menteri. Selain itu, pentingnya pemerintah dalam melindungi data pribadi adalah agar memberikan keamanan bagi masyarakat dari kebocoran data pribadi. Perlindungan hukum terhadap data privasi juga telah

diatur dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Namun regulasi yang telah diberikan kepada pemerintah belum cukup untuk melindungi data publik karena ketentuan pasal tersebut tidak memberikan sanksi pidana atas kebocoran data pribadi melainkan hanya sanksi administratif.

Kebocoran data pribadi warga negara Indonesia merupakan tantangan serius dari segi ekonomi. Kerugian negara mencapai sekitar 600 triliun rupiah, dari kasus kebocoran data pengguna BPJS. Dari kasus yang terjadi, pihak ilegal yang dikenakan pidana adalah para peretas karena hal ini merupakan tanggung jawab dari kerugian yang telah dilakukan. Informasi pribadi penduduk Indonesia dapat dijual ke sejumlah entitas, termasuk perusahaan, lembaga penegak hukum, dan pemerintah asing. Informasi KTP yang bocor dapat digunakan untuk melakukan kejahatan, seperti pencurian identitas, bahkan peneroran secara langsung.

Rusaknya kinerja perusahaan, seperti terjadi kasus kebocoran data, dapat mengakibatkan hilangnya konsumen dan turunnya pendapatan, bahkan didenda. Ketika konsumen kehilangan kepercayaan pada perusahaan, mereka mulai mencari alternatif. Hal ini bisa mengarahkan mereka kepada pesaing yang tidak mengalami serangan cyber. Contohnya pada kasus Tokopedia, terjadi kebocoran data yang menyebabkan Tokopedia digugat sebesar 100 miliar rupiah, tentu saja kepercayaan publik akan Tokopedia menurun.

Pengaturan perlindungan data telah diatur dalam beberapa undang-undang, seperti Peraturan Menteri UUD 1945, Undang-Undang Nomor 23 Tahun 2006 sebagaimana telah diubah dengan Undang-Undang Nomor 24 Tahun 2013 tentang Administrasi Kependudukan Negara Kependudukan, Undang-Undang Nomor 19

Tahun 2016 tentang Informasi dan Transaksi Elektronik, Peraturan Pemerintah Nomor 82 Tahun 2012 sebagaimana telah diubah dengan Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, Peraturan Menteri Perhubungan Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik, Deklarasi Hak Asasi Manusia, General Data Protection Regulation (GDPR) Uni Eropa, International Convention on Civil and Political Rights (ICCPR). Namun, undang-undang ini belum efektif karena masih terdapat peraturan perundang-undangan yang tumpang tindih. Masih belum ada kepastian hukum yang jelas mengenai upaya pertanggungjawaban hukum dalam mengatasi kasus kebocoran data. Pemerintah saat ini sedang melakukan upaya-upaya yang cukup baik dengan merevisi Undang-Undang Informasi dan Transaksi Elektronik, Peraturan Pemerintah, Peraturan Menteri dan sebagainya.

Data pribadi dikelompokkan berdasarkan sensitivitas data. Klasifikasi data sensitif dapat berbeda di setiap negara. Secara khusus, GDPR memberikan perlindungan khusus terhadap jenis data pribadi tertentu yang dianggap sensitif, termasuk informasi mengenai etnis, preferensi politik, agama atau kepercayaan, keanggotaan dalam organisasi perdagangan, data biometrik untuk tujuan mengidentifikasi seseorang, kesehatan, jenis kelamin, data kehidupan, dan orientasi seksual. Data sensitif tersebut dilarang untuk diproses kecuali memenuhi serangkaian persyaratan yang secara eksplisit dinyatakan dalam GDPR, termasuk persetujuan tertulis dari pemilik data dan pengumpulan data dibatasi untuk tujuan yang telah secara definitif tercantum dalam GDPR.

Dalam kemajuan pesat inovasi teknologi, dimungkinkan untuk mengkonfirmasi darurat perlindungan data pribadi, di mana lebih mudah bagi orang untuk mengakses data pribadi tanpa izin dari pemilik sebenarnya. Kasus seperti itu dapat terjadi karena kurangnya undang-undang untuk perlindungan data pribadi.

Menurut Utrecht, hukum menjamin kepastian hukum dalam interaksi sosial. Asumsi Utrecht didasarkan pada asumsi Vanikan bahwa hukum melindungi kepentingan masing-masing masyarakat agar kepentingan tersebut tidak dapat diganggu (mengandung pertimbangan bahwa kepentingan masyarakat didahulukan). Jelas dalam teori Utrecht, bahwa hukum yang baik harus melihat interaksi sosial yang timbul. Dengan adanya kasus kebocoran data, pemerintah diharapkan segera mengesahkan RUU Perlindungan Data Pribadi agar dapat memberikan manfaat hukum bagi masyarakat.

Dapat dikatakan bahwa saat ini terdapat keadaan darurat perlindungan data pribadi di tengah pesatnya perkembangan teknologi. Oleh karena itu, RUU Perlindungan Data Pribadi harus segera disahkan dan diundangkan guna menjaga kerahasiaan data pribadi warga negara Indonesia. Perlindungan Data Pribadi WNI merupakan hal mendasar yang harus diperhatikan karena percepatan pengesahan RUU Perlindungan Data Pribadi dapat menjadi solusi untuk dapat mengelola data pribadi WNI dengan baik dan benar. Sehingga RUU ini sangat penting untuk melengkapi transformasi digital guna mendapatkan jaminan hukum yang jelas terhadap kasus-kasus kebocoran data yang muncul.

KESIMPULAN

Berdasarkan uraian dan pembahasan hasil penelitian yang dilakukan, dapat ditarik beberapa kesimpulan. Peraturan mengenai

perlindungan data pribadi di Indonesia tersebar dalam beberapa peraturan yang masih bersifat umum sehingga belum ada kepastian hukum. Lebih lanjut, penerapan undang-undang perlindungan data di Indonesia yang saat ini masih dibahas di parlemen akan memberikan sisi positif bagi Indonesia dalam hal pertumbuhan ekonomi digital, pengakuan

dari negara-negara, dan pencegahan pelanggaran siber. Pertanggungjawaban atas perlindungan data pribadi harus dikenakan sanksi administratif atau pidana, kemudian penyelesaian kasus kebocoran data pribadi dapat dilakukan melalui jalur pengadilan/litigasi atau non litigasi.

DAFTAR PUSTAKA

The IJICS Vol. 5 No. 3, 246-249.

Arief, B. N. (2006). *Tindak Pidana Mayantara: Perkembangan Kajian Cybercrime di Indonesia*. Jakarta: RajaGrafindo Persada.

Arifin, R., & Atika, T. R. (2021). FACEBOOK LEAKS: HOW DOES INDONESIAN LAW REGULATE IT? *Ganesha Law Review*, 33-42.

Asosiasi Penyelenggara Jasa Internet Indonesia. (2020). *LAPORAN SURVEI INTERNET APJII*. Indonesia Survey Center.

Assifa, F. (2021). 7 Data Bocor yang Diungkap Raid Forums sebelum Diblokir Kominfo. Diambil kembali dari Kompas.com: <https://www.kompas.com/tren/read/2021/05/22/205006565/7-data-bocor-yang-diungkap-raid-forums-sebelum-diblokir-kominfo>

Council of Europe. (2001). *Convention on Cybercrime*.

Danendra, R., Handayani, I. G., Jaelani, A. K., & Najicha, F. U. (2021). LEGAL PROTECTION OF NON WAGE WORKERS' RIGHTS AFTER OMNIBUS LAW. *Jurisprudentie : Jurusan Ilmu Hukum Fakultas Syariah Dan Hukum*, 8(1), 85-99.

Djafar, W. (2019). *Perlindungan Data Pribadi Di Indonesia: Lanskap, Urgensi, Dan Kebutuhan Pembaruan*. *Jurnal Becoss* 1, no. 1, 147-54.

Hidayah, A. A., & Ezerli, S. (2020). Kasus kebocoran data semakin banyak, belanja daring paling rentan. Diambil kembali dari Lokadata: <https://amp.lokadata.id/amp/kasus-kebocoran-data-semakin-banyak-belanja-daring-paling-rentan>

Hootsuite. (2020). *Digital 2020*.

Jatmiko, L. D. (2022). Dugaan Kebocoran Data Pasien Covid-19, Aspek Keamanan Data Jadi Sorotan. Diambil kembali dari TEKNOLOGI: <https://teknologi.bisnis.com/read/20220107/84/1486379/dugaan-kebocoran-data-pasien-covid-19-aspek-keamanan-data-jadi-sorotan>

Koops, B.-J. (2014). The trouble with European data protection law. *International Data Privacy Law*, Volume 4, Issue 4, 250-261.

Kresna, M. (2019). Bagaimana Data Nasabah Kartu Kredit Diperjualbelikan. Diambil kembali dari Tirto.id: <https://tirto.id/bagaimana-data-nasabah-kartu-kredit-diperjualbelikan-djSv>

Lidwina, A. (2021). Kebocoran Data Pribadi yang Terus Berulang. Diambil kembali dari Katadata.co.id: <https://katadata.co.id/ariayudhistira/infografik/60b3bbeda4185/kebocoran-data-pribadi-yang-terus-berulang>

Malaviya, D. (2021). Rising cases of Data Leaks and the Law. *Anusandhaan - Vigyaan Shodh Patrika*, 9(1), 134-138.

- Mansur, D. M., & Gultom, E. (2005). *Cyberlaw: Aspek Hukum Informasi*. Bandung: Refika Aditama.
- Najicha, F. U., Handayani, I. G., & Hartiwiningsih. (2020). Legal Protection “Substantive Rights for Environmental Quality” on Environmental Law Against Human Rights in the Constitution in Indonesia. *Proceedings of the International Conference on Law, Economics and Health*.
- Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016
- Peraturan Pemerintah Nomor 71 Tahun 2019
- Pertiwi, W. K. (2021). Ini Dugaan Sumber Kebocoran Data 2 Juta Nasabah BRI Life. Diambil kembali dari Kompas.com: <https://tekno.kompas.com/read/2021/07/29/10010027/ini-dugaan-sumber-kebocoran-data-2-juta-nasabah-bri-life>
- Purtova, N. (2018). The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, 40-81.
- Salsabila, K., & Najicha, F. U. (2019). PENERAPAN ASAS YURIDIS DAN ASAS EKONOMIS PERPAJAKAN DI INDONESIA. *Jurnal Hukum Positum*, 6(2), 151-167.
- Undang-Undang Nomor 11 Tahun 2008
- Undang-Undang Nomor 19 Tahun 2016
- Undang-Undang Nomor 23 Tahun 2006
- Undang-Undang Nomor 24 Tahun 2013
- Warren, & Brandeis. (1890). The Right to Privacy. *Harvard Law Review* Vol. IV No. 5.