Syntax Literate: Jurnal Ilmiah Indonesia p–ISSN: 2541-0849
e-ISSN: 2548-1398
Vol. 9, No. 2, Februari 2024

TINDAK PIDANA PENYALAHGUNAAN DATA PRIBADI DALAM HUKUM SIBER INDONESIA

Desmon Trisandi, Ahmad Sofian
Fakultas Hukum, Universitas Esa Unggul, Indonesia
Email: inp.desmon@gmail.com, ahsofian@gmail.com

Abstrak

Kasus kebocoran data milik pribadi yang bersifat privasi, marak terjadi di Indonesia beberapa tahun belakangan ini. Regulasi yang mengaturnya dirasa saling tumpang tindih dan tidak terdapat keharmonisan dan sinkronisasi antara peraturan yang satu dengan peraturan yang lainnya. Penelitian ini bertujuan untuk mengkaji dan menganalisis pengaturan tindak pidana penyalahgunaan data pribadi dalam hukum siber di Indonesia dan untuk mengetahui mengenai yang seharusnya tentang perlindungan hukum data pribadi dari tindak pidana siber. Penelitian ini merupakan penelitian normatif yang bersifat deskriptif analitis. Penelitian dilakukan dengan studi kepustakaan dengan cara studi dokumen atas bahan hukum primer dan bahan hukum sekunder serta tersier. Data hasil penelitian yang diperoleh dari penelitian kepustakaan dan lapangan kemudian dianalisis secara kualitatif dan disusun secara deskriptif. Temuan penelitian pertama bahwa pengaturan tindak pidana penyalahgunaan data pribadi dalam hukum siber di Indonesia masih berdiri terpisah dalam peraturan perundang-undangan yang berbeda-beda, sehingga belum ada regulasi yang fokus mengatur secara khusus tentang perlindungan data pribadi. Aturan hukum di Indonesia tentang kebocoran data pribadi hanya mewajibkan penyelenggara sistem elektronik untuk melakukan pemberitahuan kepada pemilik data sesuai Pasal 14 Ayat (5) Peraturan Pemerintah Nomor 71 Tahun 2019 Tentang Penyelenggara Sistem dan Transaksi Elektronik. Hal yang seharusnya lebih penting dari sekedar pemberitahuan, bahwa harus dilanjutkan menjadi sebuah aturan baru yang isinya mengawal proses bocornya data pribadi yang gagal dilindungi oleh penyelenggara sistem elektronik, *sebagai sebuah kelanjutan tindakan dalam hukum acara; dengan masuknya sistem pembuktian* dimana data pribadi tersebut bocor karena memang dicuri, tidak sengaja bocor, ataupun sengaja dicuri.

Keyword: Tindak Pidana Siber, Perlindungan Data Pribadi, Privasi

Abstract

Cases of private data leaks that are private in nature have been rife in Indonesia in recent years. The regulations that govern it are felt to overlap and there is no harmony and synchronization between one regulation and another. This study aims to examine and analyze the regulation of criminal acts of misuse of personal data in cyber law in Indonesia and to find out what should be about the legal protection of personal data from cyber crimes. This research is a normative research with analytical descriptive nature. The research was conducted using library research by means of document studies on primary legal materials and secondary and tertiary legal materials. The research data obtained from library and field research were then analyzed qualitatively and compiled

How to cite:	Trisandi, D., & Sofian, A. (2024). Tindak Pidana Penyalahgunaan Data Pribadi dalam Hukum Siber Indonesia. *Syntax Literate. (9)2.* http://dx.doi.org/10.36418/syntax-literate.v9i2
E-ISSN:	2548-1398
Published by:	Ridwan Institute

descriptively. The first research finding is that the regulation of criminal acts of misuse of personal data in cyber law in Indonesia still stands separately in different laws and regulations, so there is no regulation that focuses specifically on protecting personal data. The legal rules in Indonesia regarding the leakage of personal data only oblige the electronic system operator to notify the data owner in accordance with Article 14 Paragraph (5) of Government Regulation Number 71 of 2019 concerning Electronic System and Transaction Operators. What should be more important than just a notification, that it must be continued into a new regulation containing the contents of guarding the process of leaking personal data that has failed to be protected by the electronic system operator, as a continuation of action in procedural law; with the inclusion of a proof system where the personal data is leaked because it was stolen, accidentally leaked, or deliberately stolen.

Keyword: *Cyber Crime, Personal Data Protection, Privacy*

Pendahuluan

Teknologi saat ini berkembang semakin pesat seperti memberikan akses kemudahan dan kecepatan dalam hal mengurus dokumen dan data yang kita gunakan untuk kepentingan pribadi. Setiap data pribadi penduduk disimpan dan dilindungi oleh negara (Undang-Undang, 23 C.E.). Seperti yang diatur dalam Pasal 28H ayat (4) Undang-Undang Negara Republik Indonesia Tahun 1945 yang mengatur bahwa "Setiap orang berhak mempunyai hak milik pribadi dan hak milik tersebut tidak boleh diambil alih secara sewenang-wenang oleh siapapun" dalam hal ini termasuk juga rahasia data pribadi.

Kontras dengan yang sedang marak terjadi belakangan ini beberapa contoh kasus kebocoran data pribadi dalam dalam dunia *cyber* contohnya seperti pada Mei 2021 BPJS Kesehatan mengalami kebocoran data peserta Badan Penyelenggara Jaminan Sosial (BPJS) dijual di *Raid Forums* seharga 0,15 Bitcoin (Akbar, 2021). Hal itu dilakukan oleh salah satu pengguna forum dengan nama id '*Kotz*'. Dalam pernyataannya data yang dijual termasuk data penduduk yang sudah meninggal. Ali Ghufron Mukti selaku Direktur Utama BPJS Kesehatan mengakui bahwa sebagian data yang diperjualbelikan di internet memiliki kesamaan dengan yang dimiliki oleh BPJS, tapi pihak BPJS belum bisa memastikan apakah kebocoran data tersebut adalah milik BPJS atau bukan, karena masih dilakukan penelusuran *digital forensic* (Silvia et al., 2024). Proses ini membutuhkan waktu yang cukup lama karena sangat kompleks dan melibatkan data yang jumlahnya sangat besar. Kemudian kasus selanjutnya adalah kebocoran data pada platform Cermati dan Lazada, kasus kebocoran data yang terjadi pada dua perusahaan itu beredar juga di situs *Raid Forums* sekitar akhir tahun 2020. Dalam kasus ini sebanyak 2,9 juta pengguna yang diambil dari tujuh belas perusahaan, dan sebagian besar merupakan data finansial. Sedangkan, Lazada mengalami kebocoran sejumlah 1,1 juta data. Dalam hal ini, pihak Lazada menyatakan bahwa insiden terkait keamanan data di Singapura melibatkan database khusus *redmart* yang di-*hosting* oleh penyedia layanan pihak ketiga.

Perlindungan Data Pribadi Pengguna Internet dalam peraturan perundang-undangan khususnya Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (selanjutnya disebut UU ITE), belum terdapat muatan aturan perlindungan data pribadi

secara khusus. Pada ketentuannya, terletak dalam Pasal 26 ayat (1) dan penjelasannya dalam UU ITE, yang berbunyi (Sujamawardi, 2018).

> "*Kecuali ditentukan lain oleh peraturan perundang-undangan, penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan Orang yang bersangkutan*"

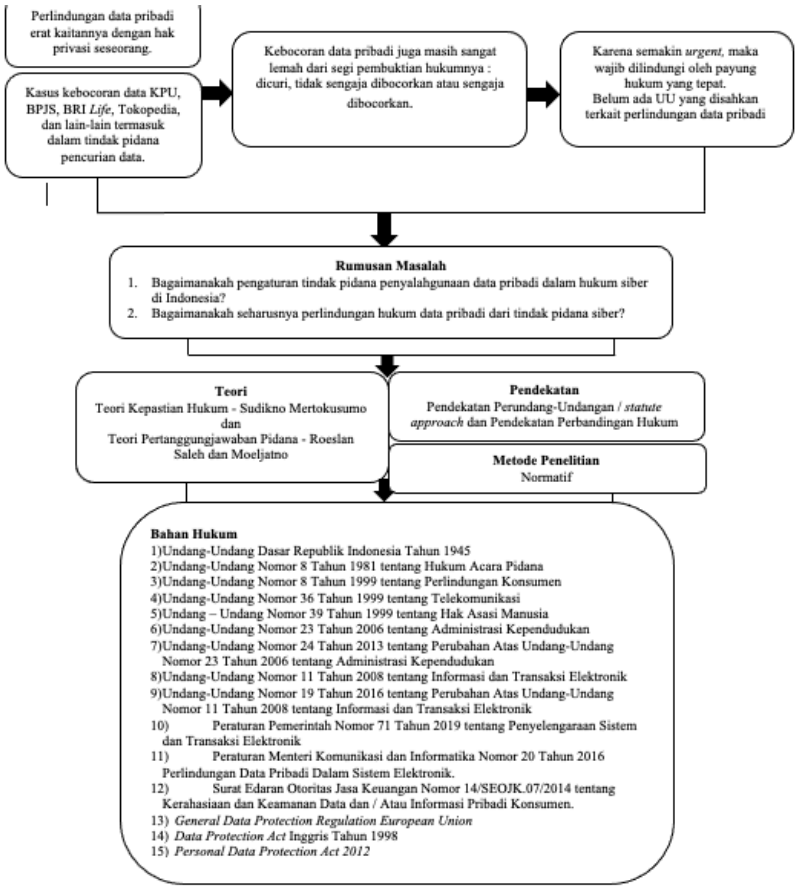
Kasus yang diangkat dalam penulisan tesis ini ialah mengenai kebocoran data pribadi milik warga negara yang termasuk dalam tindak pidana *cyber crime* atau yang kini dikenal dengan tindak pidana siber. Data pribadi yang bisa diakses tanpa persetujuan pemiliknya merupakan suatu tindakan yang disebut sebagai *cracking* (Barkatullah, 2019). *Cracking* dimaknai sebagai peretasan dengan cara merusak sebuah sistem elektronik. Selain merusak, *cracking* merupakan pembajakan data pribadi maupun *account* pribadi seseorang, sehingga mengakibatkan hilang atau berubah dan digunakan tanpa persetujuan pemilik. Oleh karena itu, penggunaan data pribadi oleh *cracker* dengan tujuan sebagaimana dimaksud di atas dapat dikategorikan sebagai bentuk pelanggaran sesuai Pasal 26 ayat (1) UU ITE.

Seseorang yang melakukan tindakan *cracking,* dapat dikatakan termasuk perbuatan dalam Pasal 30 ayat (3) UU ITE, yang berbunyi

> "*Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apapun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan*."

Peraturan terkait data pribadi di Indonesia, baik dari segi regulasi dan implementasinya, masih dirasa belum memberikan perlindungan secara komprehensif (Disemadi, 2021). Peraturan perundang-undangan yang ada, masih saling tumpang tindih dan belum mengarah pada satu persoalan khusus yang semakin dirasa penting, yakni perlindungan data pribadi yang bersifat privasi. Regulasi yang ada di Indonesia, masih belum mencangkup semua aspek yang berkaitan dengan perlindungan data pribadi, sehingga keamanan akan privasi masyarakat sebagai pemilik data pribadi masih belum tercapai.

Terkait hal tersebut, berdasarkan latar belakang permasalahan yang telah dijabarkan, maka dengan penulisan tesis ini, penulis tertarik melakukan penelitian untuk penulisan yang berjudul "Tindak Pidana Penyalahgunaan Data Pribadi Dalam Hukum Siber Indonesia.". selain itu, penelitian ini bertujuan untuk mengkaji dan menganalisis pengaturan tindak pidana penyalahgunaan data pribadi dalam hukum siber di Indonesia dan untuk mengetahui mengenai yang seharusnya tentang perlindungan hukum data pribadi dari tindak pidana siber.



Gambar 1. Bagan Kerangka Konsep
Sumber : Penulis, diolah pada tahun 2022

Metode Penelitian

Jenis Penelitian

Jenis penelitian pada penulisan tesis ini menggunakan penelitian hukum normatif. Penelitian hukum normatif ini akan dijabarkan sesuai dengan sifatnya, yaitu secara deskriptif analitis. Penelitian deskriptif memiliki karakteristik yaitu cenderung menggambarkan suatu fenomena apa adanya dengan cara menelaah secara teratur dan ketat serta mengutamakan obyektifitas secara cermat (Furchan, 2004). Penelitian hukum normatif menekankan pada penggunaan data sekunder, yang berisikan bahan hukum primer, bahan hukum sekunder, dan bahan hukum tersier yang menggunakan obyek kajian penulisan berupa sumber buku, dokumen, peraturan perundang-undangan, jurnal akademis, hasil seminar penelitian dan lain-lain yang berhubungan dengan pembahasan dalam penelitian tesis ini.

Pendekatan Penelitian

Pendekatan dalam penulisan tesis ini menggunakan pendekatan perundang-undangan yang nantinya mengkaji aturan-aturan hukum yang akan mengatur tentang perlindungan data pribadi di Indonesia sesuai asas pembentukan peraturan perundang-undangan yang baik (Munawar et al., 2021). Selain menggunakan pendekatan perundang-undangan (*statute approach*), penulis juga menggunakan pendekatan komparatif atau *comparative approach*.

Sehingga dalam penulisan tesis ini dilakukan dua pendekatan dalam metode penelitian, yaitu pendekatan perundang-undangan yang menelaah sumber-sumber peraturan perundang-undangan yang berkaitan dengan perlindungan data pribadi yang kemudian dilakukan pendekatan perbandingan hukum guna mengkaji tentang persamaan dan perbedaan dalam peraturan perundang-undangan yang ada di beberapa Negara terkait dengan perlindungan data pribadi.

Data

Data sekunder yang digunakan dalam penelitian tesis ini guna menunjang data primer yakni terdiri dari :

a. Bahan Hukum Primer
   1) Undang-Undang Dasar Republik Indonesia Tahun 1945
   2) Undang-Undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana
   3) Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen
   4) Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi
   5) Undang – Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia
   6) Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan
   7) Undang-Undang Nomor 24 Tahun 2013 tentang Perubahan Atas Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan
   8) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik
   9) Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik
   10) Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelengaraan Sistem dan Transaksi Elektronik
   11) Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 Perlindungan Data Pribadi Dalam Sistem Elektronik.
   12) Surat Edaran Otoritas Jasa Keuangan Nomor 14/SEOJK.07/2014 tentang Kerahasiaan dan Keamanan Data dan/Atau Informasi Pribadi Konsumen.
   13) *General Data Protection Regulation European Union*
   14) *Data Protection Act* Inggris Tahun 1998
   15) *Personal Data Protection Act 2012*

b. Bahan Hukum Sekunder

   Bahan hukum sekunder berupa fakta hukum, doktrin, asas-asas hukum, dan pendapat hukum dalam literatur, jurnal, hasil penelitian, dokumen, surat kabar, internet, dan majalah ilmiah tentang hukum siber dan Rancangan Undang-Undang Perlindungan Data Pribadi. Pada penulisan tesis ini, penulis lebih banyak menggunakan sumber literature buku teori terkait dengan hukum siber di Indonesia, jurnal ilmiah terkait penelitian dalam konteks perlindungan data pribadi, serta penulis juga banyak menggunakan buku terkait teori kepastian hukum dan teori pertanggungjawaban pidana yang digunakan sebagai bahan hukum sekunder, serta buku metodologi hukum normatif.

c. Bahan Hukum Tersier
   1) Kamus Bahasa Hukum
   2) Kamus Besar Bahasa Indonesia

Pengumpulan dan Pengolahan Data

Pengumpulan dan pengolahan data dalam penulisan tesis ini dilakukan dengan cara yaitu dengan mengumpulkan data sekunder penelitian yang terdiri dari bahan hukum primer, bahan hukum sekunder, dan bahan hukum tersier. Data sekunder dilakukan studi kepustakaan yaitu pengumpulan data yang diperoleh dari dokumen-dokumen kasus, literatur buku, makalah, artikel ataupun hasil penelitian dan Peraturan Perundang-undangan yang berlaku serta teori yang berkaitan dengan penulisan tesis. Data tersebut kemudian diolah dan dikaji dengan teori-teori yang ada, dan dengan pendekatan perundang-undangan dan perbandingan hukum dalam metodologi penelitian hukum normatif guna menjawab terhadap permasalahan yang akan diteliti dalam penulisan tesis.

Analisis Data

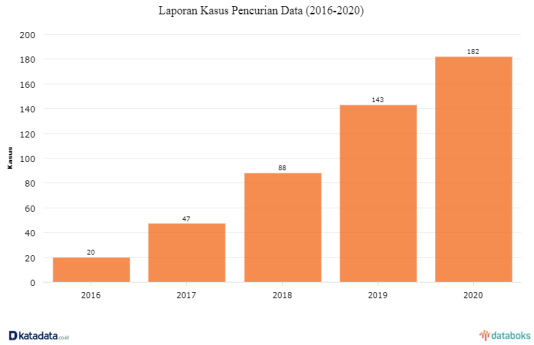
Metode analisis data yang digunakan penulis adalah kualitatif. Metode ini menghasilkan data deskriptif analisis yang menyatakan mengenai sasaran penelitian yang bersangkutan dengan baik secara tertulis maupun lisan dan berdasarkan perilaku nyata. Data yang diperoleh dalam penelitian ini dianalisis secara kualitatif yaitu analisis yang dilakukan dengan meneliti dokumen dan pustaka serta peraturan perundang-undangan terkait. Penulisan tesis ini menggunakan proses berpikir deduktif. Melalui prosedur logika deduktif, akan diperoleh kesimpulan khusus yang diarahkan pada penyusunan jawaban teoritis terhadap permasalahannya (Sunggono, 2003). Proses berfikir deduktif adalah suatu metode penalaran berfikir yang bertolak dari hal umum ditarik kesimpulan yang bersifat khusus (Susanto, 2015).

Hasil dan Pembahasan

Pengaturan Tindak Pidana Penyalahgunaan Data Pribadi Dalam Hukum Siber di Indonesia

Penyalahgunaan data pribadi dalam kasus kebocoran data pribadi di Indonesia merupakan wujud dari tindak pidana siber yang pengaturannya masih timpang tindih dan belum terfokus pada pelaku tindak pidana siber itu sendiri. Peraturan perundang-undangan di Indonesia yang mengatur tentang hukum siber, belum terfokus pada satu peraturan yang khusus sehingga diasumsikan bahwa pengaturan hukum akan hal tersebut masih belum dirasakan manfaatnya (Alfian, 2018).

Beberapa waktu belakangan terdapat informasi yang cukup menimbulkan pertanyaan besar tentang kasus kebocoran data dari diretasnya sertifikat vaksinasi milik Presiden Republik Indonesia Joko Widodo (Jayani, 2022). Dugaan bocornya data pribadi milik Presiden RI tersebut didapatkan dari aplikasi PeduliLindungi. Semenjak Pandemi Covid-19 melanda Indonesia, aplikasi PeduliLindungi yang dicanangkan oleh Pemerintah untuk penanganan dan pendataan Covid-19, merupakan aplikasi utama yang wajib dimiliki oleh warga negara, untuk kepentingan pendataan dan keperluan yang lainnya, dengan cara memasukan Nomor Induk Kependudukan. Data KTP yang harus diunggah ke dalam aplikasi PeduliLindungi tersebut, disimpan dalam aplikasi yang nantinya dipergunakan untuk keperluan, seperti untuk *check-in* ke mall atau ke fasilitas umum lainnya.



Gambar 2. Laporan Kasus Pencurian Data (2016-2020) (Jayani, 2022).
Sumber : Grafik Patroli Siber Tahun 2015-2020 katadata.com

Kasus kebocoran data yang tercatat dalam Polisi Siber sejak tahun 2016 terus meningkat hingga tahun 2020 sebanyak 81% dari tahun-tahun sebelumnya (Jayani, 2022). Kebocoran data pribadi yang diduga dicuri oleh oknum tertentu, dilaporkan masyarakat dan terus meningkat tanpa ada upaya hukum yang dapat memberi solusi dalam pencegahannya, karena sulitnya menjangkau para pelaku pencurian data pribiadi. Kondisi saat Pandemi Covid-19 juga menjadi pemicu banyaknya kasus kebocoran data milik pribadi karena segala transaksi beralih ke sistem *online* secara perlahan.

Perlindungan Hukum Data Pribadi Dari Tindak Pidana Siber

Wujud instrumen hukum untuk memberi perlindungan data pribadi kepada masyarakat saat ini di Indonesia, masih belum didapati adanya bentuk peraturan perundang-undangan yang memadai dan komprehensif. Aturan mengenai perlindungan data pribadi belum diakui sebagai wujud hak asasi manusia yang harus dihargai dan dilindungi. Undang-Undang Dasar Negara Republik Indonesia 1945 yang dengan jelas memberi penghormatan dan menegakkan HAM, namun dalam ranah perlindungan data pribadi sebagai ranah privasi, tidak diatur secara tegas. Ketentuan tersebut hanya tersirat pada Pasal 28H Ayat (4) Undang-Undang Dasar Negara Republik Indonesia 1945, bahwa negara memberikan kebebasan untuk menyimpan informasi dan perlindungan atas data dan informasi yang melekat kepadanya.

Pentingnya untuk segera disahkannya RUU Perlindungan data Pribadi karena pada kasus kebocoran data pribadi yang seharusnya bersifat privasi, kini sudah diperjualbelikan oleh oknum tidak bertanggungjawab yang hanya mengeruk keuntungan pribadi saja, kebocoran data pribadi tersebut baik untuk kepentingan kebutuhan data, bahkan sampai dengan kebutuhan akan rekaman medis juga telah diperjual belikan pada situs *Dark Web*. Data pribadi yang bocor diperjualbelikan dalam laman situs yang tidak terpantau atau illegal (Annur, 2022).

Penanganan yang dilakukan sebagai upaya represif oleh pihak berwenang, dalam hal ini juga dilakukan oleh Kementerian Komunikasi dan Informasi. Sejak tahun 2019 sampai dengan tahun 2021, Kementerian Komunikasi dan Informasi telah menangani kasus dugaan kebocoran data pribadi terhadap Penyelenggara Sistem Elektronik sebanyak tiga puluh enam penyelenggara (Doni, 2022). Sebanyak empat peneyelenggara sistem elektronik telah diberi sanksi teguran tertulis, delapan belas diberi rekomendasi teknis peningkatan tata kelola dan sistem elektronik, dan sisanya ada sembilan pihak penyelenggara sistem elektronik yang sedang dalam proses untuk diberikan sanksi akhir. Disahkannya rancangan undang-undang menjadi undang-undang untuk perlindungan data pribadi ini secara otomatis akan membantu pihak Pemerintah

dalam memaksimalkan sistem pengawasan dan penindakan terhadap adanya kasus kebocoran data pribadi. Selain dari pihak Pemerintah, dalam hal perlindungan data pribadi tentunya tidak jauh dari partisipasi masyarakat Indoensia sendiri.

Aturan dalam peraturan perundang-undangan yang mengatur tentang perlindungan data pribadi yang sudah ada, diharapkan menjadi acuan untuk mencapai Undang-Undang Perlindungan data Pribadi yang ideal setelah ada sinkronisasi dan harmonisasi terhadap aturan yang satu dengan yang lainnya. Sumber hukum yang saat ini terkait perlindungan data pribadi di Indonesia, tertuang dalam Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik. Pasal 1 Angka 1 Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik mengatur bahwa (Anggraeni, 2018):

> *"yang dimaksud dengan data pribadi adalah data perseorangan tertentu yang disimpan, dirawat, dan dijaga kebenaran serta dilindungi kerahasiaannya."*

Pembahasan

Pertama, pengaturan tentang data pribadi dan tindak pidana penyalahgunaan data pribadi dalam hukum siber di Indonesia masih berdiri terpisah dalam peraturan perundang-undangan yang berbeda-beda, sehingga belum ada regulasi yang fokus mengatur secara khusus tentang perlindungan data pribadi. Data pribadi merupakan hak milik yang melekat pada setiap individu, dan atas kepemilikannya itu diatur dalam Pasal 28 H Ayat (4) Undang-Undang Dasar Republik Indonesia Tahun 1945 bahwa setiap warga Negara Indonesia dijamin oleh Undang-Undang, atas hak milik pribadi dan hak milik tersebut tidak boleh diambil alih secara sewenang-wenang oleh siapapun. Hak-hak konsumen dalam transaksi elektronik, jelas diatur dalam Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen bahwa konsumen berhak atas keamanan termasuk juga dilindungi atas informasi data pribadinya. Data pribadi yang bersifat privasi dalam dunia perbankan dan telekomunikasi juga diatur dalam regulasi yang berdiri secara terpisah, yakni pada Pasal 42 Ayat (1) Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi dan Pasal 40 Ayat (1) Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan. Pengertian atau definisi tentang data pribadi dijabarkan melalui Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, namun yang mengatur tentang kriteria data perorangan, justru dijabarkan dalam dalam Pasal 84 ayat (1) Undang-Undang Nomor 24 Tahun 2013 tentang Perubahan Atas Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan. Peraturan perundang-undangan yang mengatur tentang data pribadi, justru tidak didapati pada satu wadah yang khusus mengaturnya, melainkan berdiri secara terpisah-pisah, baik pengertiannya, kriterianya ataupun ketentuan lainnya. Hal inilah yang menjadi dasar, bahwa di Indonesia belum ada payung hukum yang tepat dalam rangka memberikan perlindungan data pribadi yang bersifat privasi kepada warga negaranya. Pengaturan perlindungan data pribadi dari tindak pidana penyalahgunaan data pribadi dalam hukum siber di Indonesia masih belum ditemukan sinkronisasi dan harmonisasi peraturan perundang-undangan tentang perlindungan data pribadi. Ketentuan akan aturan yang ada tentang perlindungan data pribadi masih terbagi-bagi dalam kewenangan antar Lembaga Negara yaitu antara Kementrian Komunikasi dan Informasi dengan produk hukum berupa Undang-Undang Nomor 19 Tahun 2016 tentang

Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dan Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik serta Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelengaraan Sistem dan Transaksi Elektronik, sehingga belum ada payung hukum yang tepat dan komprehensif untuk mengatur terkait tindak pidana penyalahgunaan data pribadi sebagai bentuk perlindungan privasi.

Kedua, perlindungan hukum data pribadi dari tindak pidana siber di Indonesia seharusnya dapat mengadopsi dari peraturan perlindungan data pribadi yang ada di dunia. Sebagai contoh, Indonesia dapat mengadopsi ketentuan regulasi perlindungan data pribadi yang diformulasikan oleh *General Data Protection Regulation European Union* dimana lingkup rumusan aturan dalam regulasi dapat meliputi (1) Subyek pemilik data pribadi; (2) Lembaga sah yang berdiri sendiri atau bersama-sama menentukan tujuan perlindungan data pribadi; (3) wujud kegiatan yang dilakukan Lembaga dalam melakukan tujuan pemrosesan data pribadi; (4) Pihak yang memiliki kewenangan untuk melakukan penyelidikan, pengaksesan, dan berhak untuk menghalangi pengiriman data pribadi kepada yang bukan berhak atas akses data pribadi. Rancangan Undang-Undang Perlindungan Data Pribadi di Indonesia harus lebih menekankan pada klasifikasi dan *jenis-jenis yang termasuk dalam pelanggaran* tindak pidana pencurian data pribadi; hukum acara dalam *penyelesaian sengketa* pada kasus kebocoran data pribadi; serta wujud *tanggung jawab pidana* (pertanggungjawaban pidana) bagi siapapun yang melanggar privasi dalam ketentuan pengaksesan data pribadi.

Kesimpulan

Secara keseluruhan, konteks hukum siber dan perlindungan data pribadi di Indonesia masih terfragmentasi dan belum memiliki regulasi yang menyeluruh. Keterpisahan regulasi mengenai data pribadi dan tindak pidana penyalahgunaannya menimbulkan kekosongan hukum yang perlu diatasi untuk melindungi hak privasi individu sesuai dengan Pasal 28 H Ayat (4) Undang-Undang Dasar Republik Indonesia Tahun 1945. Perlindungan hukum terhadap data pribadi seharusnya disinkronkan dan diharmonisasikan dalam satu payung hukum komprehensif. Adopsi ketentuan regulasi perlindungan data pribadi dari aturan internasional, seperti General Data Protection Regulation European Union, dapat menjadi landasan untuk merumuskan undang-undang perlindungan data pribadi yang lebih efektif dan sesuai dengan perkembangan teknologi. Diperlukan penekanan pada klasifikasi pelanggaran tindak pidana terkait data pribadi, mekanisme penyelesaian sengketa, dan penetapan pertanggungjawaban pidana sebagai upaya penguatan perlindungan privasi dalam era digital di Indonesia.

BIBLIOGRAFI

Akbar, C. (2021). *Syailendra Persada, 6 Kasus Kebocoran Data Pribadi Di Indonesia*. https://nasional.tempo.co/read/1501790/6-kasus-kebocoran-data-pribadi-di-indonesia

Alfian, M. (2018). Penguatan Hukum Cyber Crime di Indonesia dalam Perspektif Peraturan Perundang-Undangan. *Kosmik Hukum*, *17*(2).

Anggraeni, S. F. (2018). Polemik Pengaturan Kepemilikan Data Pribadi: Urgensi Untuk

Harmonisasi Dan Reformasi Hukum Di Indonesia. *Jurnal Hukum & Pembangunan*, *48*(4), 814–825.

Annur, C. M. (2022). *Pencurian Data Pribadi Dalam Pusaran Bisnis Fintech Ilegal*. Katadata.Com. https://katadata.co.id/ariayudhistira/analisisdata/609a43a46aa5e/pencurian-data-pribadi-dalam-pusaran-bisnis-fintech-ilegal

Barkatullah, A. H. (2019). *Hukum Transaksi Elektronik di Indonesia: sebagai pedoman dalam menghadapi era digital Bisnis e-commerce di Indonesia*. Nusamedia.

Disemadi, H. S. (2021). Urgensi regulasi khusus dan pemanfaatan artificial intelligence dalam mewujudkan perlindungan data pribadi di Indonesia. *Jurnal Wawasan Yuridika*, *5*(2), 177–199.

Doni. (2022). *Memastikan Data Pribadi Aman*. Indonesia.Go.Id. https://www.kominfo.go.id/content/detail/37332/memastikan-data-pribadi-aman/0/artikel

Furchan. (2004). *Pengantar Penelitian dan Pendidikan*. Pustaka Pelajar Offset.

Jayani, D. H. (2022). *Pencurian Data Pribadi Makin Marak Kala Pandemi*. https://databoks.katadata.co.id/datapublish/2021/09/07/pencurian-data-pribadi-makin-marak-kala-pandemi

Munawar, M., Marzuki, M., & Affan, I. (2021). Analisis Dalam Proses Pembentukan Undang-Undang Cipta Kerja Perpspektif Undang-Undang Nomor 12 Tahun 2011 Tentang Pembentukan Peraturan Perundang-Undangan. *Jurnal Ilmiah METADATA*, *3*(2), 452–468.

Silvia, A. F., Saputra, W., Sunaryo, H., & Sinlae, F. (2024). Analisis Keamanan Data Pribadi pada Pengguna BPJS Kesehatan: Ancaman, Risiko, Strategi Kemanan (Literature Review). *Nusantara Journal of Multidisciplinary Science*, *1*(6), 201–207.

Sujamawardi, L. H. (2018). Analisis Yuridis Pasal 27 ayat (1) Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. *Dialogia Iuridica*, *9*(2).

Sunggono, B. (2003). *Metodologi penelitian hukum*.

Susanto, A. F. (2015). *Penelitian hukum: transformatif-partisipatoris*.

Undang-Undang. (23 C.E.). *tahun 2006 tentang Administrasi Kependudukan*.