

PERLINDUNGAN HUKUM TERHADAP KORBAN KEBOCORAN DATA PRIBADI (STUDI KASUS DI KOTA DENPASAR)

A.A. Ngurah Oka Yudistira Darmadi, Fakultas Hukum Universitas Udayana,
e-mail: oka_yudisitira@unud.ac.id
Nyoman Satyayudha Dananjaya, Fakultas Hukum Universitas Udayana,
e-mail: satyayudha@unud.ac.id

doi: <https://doi.org/10.24843/KS.2023.v11.i05.p13>

ABSTRAK

Studi ini bertujuan untuk mengetahui dan memberikan pengetahuan mengenai perlindungan hukum secara umum serta langkah konkret bagi korban serta yang data pribadinya bocor. Penelitian ini disusun menggunakan jenis metode penelitian hukum empiris dengan lokasi penelitian dilakukan di Kantor legalpartner.id, Asosiasi Profesional Perlindungan Data Indonesia, dan Kantor Advokat di Denpasar. Data yang digunakan dalam penelitian ini berupa data primer dan data sekunder. Data primer yang dikumpulkan dalam bentuk hasil wawancara dengan beberapa informan. Teknik penentuan informan tersebut menggunakan penentuan sampel secara sengaja (purposive sampling). Sedangkan, data sekunder terbagi atas bahan hukum primer, sekunder, dan tersier. Data-data penelitian dikumpulkan dengan menggunakan teknik observasi, wawancara, dan dokumentasi. Data yang telah terkumpul kemudian diolah secara kualitatif. Hasil studi menunjukkan bahwa perlindungan umum data pribadi didasarkan pada ketentuan pada Pasal 28G ayat (1) UUD NRI Tahun 1945. Kewajiban pemerintah tersebut kemudian diderivasikan melalui beberapa peraturan perundang-undangan di Indonesia. Selain itu, langkah konkret yang dapat diambil oleh korban ketika datanya bocor adalah dengan memilih jalur hukum yang disediakan berupa penanganan perkara pada ranah perdata, administratif, dan/atau pidana sesuai jalur hukum yang dipilih korban atau dengan kata lain pengajuan perkara tersebut dilakukan secara litigasi atau non litigasi.

Kata Kunci: *Data Pribadi, Korban, Perlindungan Hukum.*

ABSTRACT

This study aims to find out and provide knowledge about legal protection in general as well as concrete steps for victims and whose personal data is leaked. and the Advocate's Office in Denpasar. The data used in this study are primary data and secondary data. Primary data collected in the form of interviews with several informants. The technique of determining the informants uses purposive sampling. Meanwhile, secondary data is divided into primary, secondary, and tertiary legal materials. The research data were collected using observation, interview, and documentation techniques. The data that has been collected is then processed qualitatively. The results of the study show that the general protection of personal data is based on the provisions of Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia. The government's obligations are then derived through several laws and regulations in Indonesia. In addition, a concrete step that can be taken by the victim when the data is leaked is to choose the legal route provided in the form of handling cases in the civil, administrative, and/or criminal domains according to the legal route chosen by the victim or in other words the submission of the case is carried out by litigation or non-litigation.

Key Words: *Personal Data, Victims, Legal Protections.*

1. Pendahuluan

1.1 Latar Belakang Masalah

Perkembangan teknologi selalu menunjukkan sebuah inovasi baru dalam memperoleh, menyimpan, memanipulasi bahkan mentransmisikan data secara nyata (*real time*), luas dan kompleks. Perkembangan tersebut mendorong untuk pengumpulan berbagai data, tidak lagi melihat mana yang penting melainkan menghimpun seluruh data yang ada dan mungkin untuk dihimpun. Ketergantungan akan teknologi, menyebabkan hampir seluruh hal bergantung pada teknologi, salah satunya menghimpun data pribadi milik seseorang yang nantinya akan disimpan ke dalam *data base*. Di sisi lain kecepatan daripada pendistribusian data yang kurang daripada 1 menit dengan penyebaran yang masif telah mempermudah tindak pidana dilakukan contohnya dengan terjadinya *skimming* karena tersalinnya data dan informasi ATM, pinjaman *online* dengan mekanisme seolah seseorang yang dicuri datanya meminjam dan terlambat membayar sehingga terintimidasi, serta adanya penipuan transportasi *online* dengan pengambilan nomor ponsel.¹

Tidak semua yang diharapkan terjadi. Data pribadi yang dihimpun oleh beberapa orang membuat tidak sedikit orang untuk menggunakannya dalam hal yang tidak baik. Penggunaan data pribadi seseorang digunakan untuk kepentingan pribadinya sendiri, seperti meminjam dana di salah satu jasa keuangan, seperti yang dialami oleh Andi Karina. Andi Karina menyebutkan bahwa ia menerima somasi tagihan kartu kredit dari salah satu Bank di Indonesia yang korban sendiri tidak pernah mengajukan sebelumnya. Somasi tagihan kartu kredit yang diterima tentu membuat korban terkejut, dikarenakan korban tidak pernah memiliki kartu kredit ataupun memiliki rekening di Bank tersebut.² Sebagai hak yang melekat pada diri seseorang, perdebatan mengenai pentingnya perlindungan terhadap hak privasi seseorang. Sejatinya, perkembangan teknologi harus diikuti pula dengan perkembangan terhadap perlindungan atas hak privasi seseorang. Namun, perkembangan mengenai pengaturan terhadap perlindungan data pribadi seseorang di Indonesia masih pada tahap rancangan undang-undang saja.

Salah satu upaya dalam Perlindungan Data Pribadi Masyarakat Indonesia adalah dengan menciptakan regulasi atau peraturan yang menjadi landasan yuridis dalam hal ini perlindungan data pribadi seperti Undang-Undang Nomor 17 Tahun 2007 tentang Rencana Pembangunan Jangka Panjang 2005-2025. Di dalam UU 17/2007 ini kemudian mengatur lebih lanjut perihal perwujudan bangsa yang berdaya saing melalui pemanfaatan IPTEK dengan peraturan yuridis yang berkaitan dengan perlindungan privasi. Pengesahan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (selanjutnya disebut UU PDP) pada 20 September 2022 menandakan memang terdapat adanya kesadaran pemerintah dalam hal melindungi data pribadi masyarakatnya.

Adapun sebelum Menyusun jurnal ilmiah ini, penulis menemukan jurnal dengan tema yang sama ditulis oleh Sahat Maruli Tua Situmeang pada Jurnal SASI tahun 2019 dengan judul Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna

¹ Situmeang, Sahat Maruli Tua. Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna dalam Perspektif Hukum Siber. *Jurnal SASI Volume 27 Nomor 1* (2019): 38-52. DOI: 10.47268/sasi.v27i1.394

² Reza Hadyan, 2021, "Tagihan Palsu dan Rentannya Penyalahgunaan Data Pribadi", URL: <https://teknologi.bisnis.com/read/20210425/84/1385873/tagihan-palsu-dan-rentannya-penyalahgunaan-data-pribadi>, diakses pada 15 Desember 2021, Pukul 17.50 WITA.

dalam Perspektif Hukum Siber, yang menjadi perbedaan dengan tulisan ilmiah ini adalah terletak pada metode penelitian yang digunakan, yakni tulisan ilmiah tersebut menggunakan metode penelitian hukum normatif, sedangkan tulisan ilmiah ini menggunakan metode penelitian hukum empiris.

1.2 Rumusan Masalah

Berdasarkan uraian latar belakang di atas, maka rumusan masalah yang dapat penulis angkat ialah:

1. Bagaimana bentuk perlindungan hukum secara umum bagi korban yang data pribadinya bocor?
2. Bagaimana langkah kongkrit yang dapat diambil oleh korban yang data pribadinya bocor?

1.3 Tujuan Penulisan

Adapun tujuan dari penelitian ini adalah untuk mengetahui dan memberikan pengetahuan mengenai perlindungan hukum secara umum bagi korban yang data pribadinya bocor serta untuk mengetahui dan memberikan pengetahuan mengenai langkah kongkrit

2. Metode Penelitian

Studi ini memakai metode penelitian hukum empiris dengan bertitik tolak dengan adanya *gap* atau celah penerapan hukum antara *das sollen* dengan *das sein*, yakni penyelesaian perkara kebocoran data pribadi pengguna layanan sebagaimana diatur dalam Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik berikut aturan pelaksanaannya serta peraturan parsial dan sektoral lainnya yang terkait data pribadi para *adressat*-nya atau subyek yang dituju dalam undang-undang terkait berbanding terbalik dengan semakin marak serta meningkatnya kebocoran data pribadi yang dialami masyarakat Indonesia pada waktu belakangan ini. Penelitian terhadap *gap* tersebut dilakukan dengan mengambil lokasi penelitian di Kantor legalpartner.id, Asosiasi Profesional Perlindungan Data Indonesia, dan Kantor Advokat di Denpasar. Wilayah penelitian secara keseluruhan adalah Kota Denpasar. Peneliti menentukan wilayah berdasarkan pertimbangan untuk mempersempit ruang lingkup penelitian dan dikarenakan permasalahan yang diteliti merupakan permasalahan yang bersifat homogen sehingga dapat dijadikan indikator bagi kondisi yang sama dalam wilayah yang lebih luas. Sifat penelitian ini adalah kualitatif yang artinya suatu objek, fenomena, atau *setting social* terejawantah dalam suatu tulisan yang bersifat naratif atau terangkai dengan kata.

Data penelitian yang digunakan dalam penelitian ini adalah data primer dan data sekunder. Data primer dalam penelitian ini berupa hasil wawancara yang telah dilakukan dengan beberapa informan yang terkait dengan topik penelitian. Sedangkan, data sekunder yang digunakan terdiri atas tiga jenis yakni bahan hukum primer, sekunder, dan tersier. Data-data tersebut dikumpulkan melalui teknik observasi, wawancara, dan dokumentasi. Terhadap data primer, para informan ditentukan dengan menggunakan teknik *purposive sampling* atau penelitian yang terdapat tujuan atau masalah yang tengah diteliti atau dengan kata lain informan dipilih secara sengaja dengan kapasitas yang mempunyai pengetahuan dan informasi terkait topik penelitian. Analisis data yang telah terkumpul dilakukan secara kualitatif

untuk selanjutnya dideskripsikan berdasarkan penilaian yang sesuai dengan aturan hukum secara nasional.

3. Hasil dan Pembahasan

3.1 Bentuk Perlindungan Hukum Secara Umum Bagi Korban yang Data Pribadinya Bocor

Teknologi sebagai suatu bentuk inovasi dewasa ini telah mampu melakukan pengumpulan, penyimpanan, pembagian, dan penganalisaan data. Aktivitas tersebut telah mengakibatkan berbagai sektor kehidupan memanfaatkan sistem teknologi informasi, seperti penyelenggaraan *electronic commerce (e-commerce)* dalam sektor perdagangan/bisnis, *electronic education (e-education)* dalam bidang pendidikan, *electronic government (e-government)* dalam bidang pemerintahan, serta perkembangan di bidang industri lainnya.

Seiring dengan pesatnya teknologi dalam lingkungan masyarakat, isu mengenai pentingnya perlindungan data pribadi mulai muncul dan menguat, baik dalam masyarakat internasional maupun nasional. Dalam konteks internasional, beberapa instrumen hukum internasional mengatur prinsip-prinsip privasi data yang diakui secara internasional dan dijadikan sebagai fondasi hukum perlindungan data yang modern. Adapun instrumen hukum internasional yang dibentuk guna memberikan aturan mengenai data pribadi diantaranya seperti *Organization for Economic Co-operation and Development (OECD) Privacy Guidelines*, *European Convention for the Protection of Human Rights*, dan *The European Union DP Directive*. Beberapa di antara instrument tersebut kemudian diatur secara lebih lanjut secara khusus melalui instrumen hukum nasional di beberapa negara, dan beberapa instrument lain tetap berkedudukan sebagai kaidah aturan umum mengenai data pribadi.³

Dalam khazanah sistem hukum nasional, urgensi perlindungan data pribadi secara tidak langsung sesungguhnya telah terakodomir dalam Pembukaan Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 yang menyebutkan bahwa Pemerintah Negara Indonesia mempunyai kewajiban konstitusional melindungi segenap bangsa Indonesia dan seluruh tumpah darah Indonesia dan untuk memajukan kesejahteraan umum, mencerdaskan kehidupan bangsa, dan ikut melaksanakan ketertiban dunia yang berdasarkan kemerdekaan, perdamaian abadi dan keadilan sosial. Dalam konteks perkembangan teknologi informasi dan komunikasi, tujuan bernegara tersebut diwujudkan dalam bentuk perlindungan data pribadi dari setiap penduduk atau warga negara Indonesia

Kewajiban Pemerintah Negara Indonesia dalam memberikan perlindungan data pribadi didasarkan pada ketentuan pada Pasal 28G ayat (1) UUD NRI Tahun 1945 menyebutkan bahwa:

“Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, harta benda yang di bawah kekuasaannya serta berhak atas rasa aman serta berhak atas perlindungan dari ancaman rasa ketakutan untuk berbuat sesuatu atau tidak berbuat sesuatu yang merupakan hak asasi.”

³ Wulansari, e.m., 2021. Kosep Perlindungan Data Pribadi Sebagai Aspek Fundamental Normdalam Perlindungan Terhadap Hak Atas Privasi Seseorang di Indonesia. *jurnal surya kencana dua: dinamika masalah hukum dan keadilan*, 7(2), pp.265-289.

Meskipun tidak secara eksplisit menyebut mengenai privasi dan perlindungan data pribadi, namun berdasarkan ketentuan tersebut mengisyaratkan bahwa perlindungan diri pribadi merupakan salah satu bentuk perwujudan tujuan negara yang harus dilaksanakan oleh negara Indonesia, termasuk untuk melindungi hak-hak pribadi atau individual di dalam masyarakat sehubungan dengan pengumpulan, pemrosesan, penyelenggaraan, penyebarluasan data pribadi.⁴

Kewajiban negara Indonesia untuk memberikan perlindungan hak asasi manusia khususnya dalam hal data pribadi masyarakat Indonesia sesungguhnya secara implisit juga telah diderivikasikan melalui beberapa peraturan perundang-undangan yang di dalamnya mengatur mengenai privasi dan perlindungan data pribadi dalam berbagai bidang. Dalam Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (selanjutnya disebut UU ITE), pada Pasal 26 ayat (1) menyebut "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." Dijelaskan dalam Penjelasan pasal *a quo* bahwa:

"Dalam pemanfaatan Teknologi Informasi, perlindungan data pribadi merupakan salah satu bagian dari hak pribadi (*privacy rights*). Hak pribadi mengandung pengertian sebagai berikut:

- a. Hak pribadi merupakan hak untuk menikmati kehidupan pribadi dan bebas dari segala macam gangguan.
- b. Hak pribadi merupakan hak untuk dapat berkomunikasi dengan Orang lain tanpa tindakan memata-matai.
- c. Hak pribadi merupakan hak untuk mengawasi akses informasi tentang kehidupan pribadi dan data seseorang."

Pengaturan mengenai perlindungan data pribadi juga diatur secara lebih lanjut melalui pembentukan Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem Dan Transaksi Elektronik yang kini telah diganti dengan Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem Dan Transaksi Elektronik (selanjutnya disebut dengan PP PTSE). Bahwa di dalam peraturan tersebut secara autentik memberikan definisi data pribadi yaitu "setiap data tentang seseorang baik yang teridentifikasi dan/atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui Sistem Elektronik dan / atau non elektronik."

Pada galibnya, setiap penyelenggara sistem elektronik baik perseorangan, penyelenggara negara, badan usaha, maupun masyarakat yang menyediakan, mengelola, dan/atau mengoperasikan sistem elektronik secara sendiri-sendiri maupun bersama-sama kepada pengguna sistem elektronik untuk keperluan dirinya dan/atau keperluan pihak lain wajib untuk melaksanakan prinsip perlindungan data pribadi yang meliputi: a. perolehan dan pengumpulan; b. pengolahan dan penganalisisan; c. penyimpanan; d. perbaikan dan pembaruan; e. penampilan, pengumuman, transfer, penyebarluasan, atau pengungkapan; dan/ atau f. penghapusan atau pemusnahan. Segala pemrosesan data pribadi harus melibatkan persetujuan yang sah dari pemilik data pribadi untuk 1 (satu) atau beberapa tujuan tertentu yang telah disampaikan kepada pemilik data pribadi. Ketika terjadi kegagalan perlindungan data pribadi yang meliputi seluruh aspek pemrosesan, pembentuk undang-undang mengamanatkan

⁴ Yuniarti, S., 2019. Perlindungan hukum data pribadi di Indonesia. *Business Economic, Communication, and Social Sciences (BECOSS) Journal*, 1(1), pp.147-154.

bahwa Penyelenggara Sistem Elektronik wajib memberitahukan secara tertulis kepada pemilik data pribadi tersebut (*vide* Pasal 1 angka 4 UU ITE *jo.* Pasal 14 ayat (1) sampai dengan Pasal 14 ayat (5) PP Nomor 71 Tahun 2019 PP PSTE).

Dipertegas kembali dalam Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik (Permenkominfo PDPSE), Pemilik data pribadi berhak atas kerahasiaan data pribadinya (*vide* Pasal 26 huruf a Permenkominfo PDPSE). Apabila terjadi kegagalan perlindungan data pribadi, si pemilik berhak untuk mengajukan pengaduan dalam rangka penyelesaian sengketa Data Pribadi atas kegagalan perlindungan kerahasiaan Data Pribadinya oleh Penyelenggara Sistem Elektronik kepada Menteri terkait (*vide* Pasal 26 huruf b Permenkominfo PDPSE). Penyelenggara Sistem Elektronik sebagai pihak penyimpan data pribadi mempunyai kewajiban menjaga kebenaran, keabsahan, kerahasiaan, keakuratan dan relevansi serta kesesuaian dengan tujuan perolehan, pengumpulan, pengolahan, penganalisisan, penyimpanan, penampilan, pengumuman, pengiriman, penyebarluasan, dan pemusnahan Data Pribadi. Seperti telah disebut sebelumnya, ketika terjadi kegagalan perlindungan data pribadi, Penyelenggara Sistem Elektronik harus memberikan notifikasi tertulis kepada pemilik data pribadi atas kegagalan perlindungan data pribadi terhadap dirinya.

3.2 Langkah Konkret yang Dapat Diambil Oleh Korban yang Data Pribadinya Bocor

Pengaturan terhadap data pribadi di Indonesia yang masih secara parsial dan sektoral ternyata tidak memberikan perlindungan hukum yang komprehensif ketika terjadi kebocoran data. Ketiadaan pengaturan perundang-undangan tersebut belum secara khusus mengatur langkah konkret yang dapat diambil oleh korban. Konstataasi tersebut menyebabkan masyarakat memiliki ketakutan dan kebingungan apakah memberikan data pribadinya atau tidak, tapi untuk beberapa hal mau tidak mau harus memberikan data pribadinya. Oleh karena itu, beberapa advokat maupun pihak lain menggunakan beberapa ketentuan dan instrumen hukum yang berlaku guna tetap menyelesaikan perkara tersebut.

Data pribadi sendiri dapat disebut sebagai suatu data yang bersifat sensitif apabila data tersebut berkaitan langsung dengan identitas seseorang⁵. Perlindungan terhadap data pribadi berkaitan erat dengan konsep hak privasi. Privasi menurut Kamus Besar Bahasa Indonesia diartikan sebagai kebebasan atau keleluasaan pribadi. Pengumpulan dan penyebarluasan data pribadi merupakan suatu pelanggaran atas privasi karena bertentangan dengan kebebasan dan keleluasaan untuk menentukan akan memberikan atau tidak data pribadi yang bersangkutan. Hak privasi telah berkembang menjadi hak privat setiap orang sehingga dapat digunakan merumuskan suatu hak yang peruntukannya melindungi data pribadi⁶.

Tendensi pelanggaran data pribadi tidak hanya terjadi melalui media konvensional, tetapi juga acapkali terjadi secara daring misalnya yang kerap terjadi adalah ketika akan menggunakan suatu layanan aplikasi, para pengguna diminta

⁵ Sautunnida, Lia. "Urgensi Undang-Undang Perlindungan Data Pribadi di Indonesia: Studi Perbandingan Hukum Inggris dan Malaysia." *Kanun Jurnal Ilmu Hukum* 20, no. 2 (2018): 369-384. 372.

⁶ Ayu D., Ananthia, Titis Anindyajati, dan Abdul Ghoffar, 2019. "Perlindungan Hak Privasi atas Data Diri di Era Ekonomi Digital". *Hasil Penelitian*. Kepaniteraan dan Sekretariat Jenderal Mahkamah Konstitusi. 24.

untuk memberikan persetujuan atas syarat dan kondisi (*term & conditions*) layanan aplikasi tersebut yang meminta akses data yang bersifat pribadi dari pengguna seperti misalnya nomor telepon yang ada di kontak⁷. Para pengguna biasanya tidak mempunyai pilihan lain selain menyetujui permintaan akses dari penyedia layanan tersebut karena jika tidak, maka pengguna tidak akan dapat menggunakan layanan. Selain itu, terdapat pula contoh kegiatan lain yang diketahui sebagai pelanggaran atas hak privasi seperti *digital dossier* atau pengumpulan data pribadi secara masal, pelaksanaan program *e-health* dan kegiatan komputasi awan (*cloud computing*)⁸.

Pentingnya perlindungan data pribadi disebabkan data pribadi merupakan suatu aset atau komoditas yang bernilai ekonomi tinggi⁹. Diatur dalam Pasal 1 angka 22 Undang-Undang Nomor 24 Tahun 2013 tentang Perubahan atas Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan (selanjutnya disebut UU Adminduk) bahwa "Data Pribadi adalah data perseorangan tertentu yang disimpan, dirawat, dan dijaga kebenaran serta dilindungi kerahasiaannya". Lebih lanjut dalam Pasal 84 UU Adminduk bahwa data pribadi penduduk yang harus dilindungi meliputi:

- 1) keterangan tentang cacat fisik dan/atau mental;
- 2) sidik jari;
- 3) iris mata;
- 4) tanda tangan; dan
- 5) elemen data lainnya yang merupakan aib seseorang.

Penggunaan data pribadi dalam UU Adminduk terbatas hanya diberikan kepada petugas provinsi dan petugas instansi pelaksana. Petugas yang diberikan akses data tersebut juga dilarang menyebarluaskan Data Pribadi yang tidak sesuai dengan kewenangannya (*vide* Pasal 86 ayat (1) dan ayat (1a) UU Adminduk). Petugas mana yang melakukan pelanggaran atas larangan tersebut akan diancam dengan pidana penjara paling lama 2 (dua) tahun dan/atau denda paling banyak Rp25.000.000,00 (dua puluh lima juta rupiah) (*vide* Pasal 95A UU Adminduk). Dilansir dari *Privacy International*, selain data pribadi yang tersebut dalam UU Adminduk, adapun pula pengaturan mengenai data pribadi secara langsung atau tidak langsung mengarah pada perlindungan hukum data pribadi yakni beberapa diantaranya Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan (UU Perbankan); Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen (UU Perlindungan Konsumen); Undang-Undang Nomor 23 Tahun 1999 tentang Bank Indonesia (UU Bank Indonesia); Undang-Undang Nomor 31 Tahun 1999 tentang Pemberantasan Tindak Pidana Korupsi (UU Pemberantasan Korupsi); Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi (UU Telekomunikasi), dan Undang-Undang Nomor 29 Tahun 2004 tentang Praktik Kedokteran (UU Praktik Kedokteran); Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik (UU KIP); dan lain-lain¹⁰.

⁷ Fathur, Muhammad. "Tanggung Jawab Tokopedia Terhadap Kebocoran Data Pribadi Konsumen." In *National Conference on Law Studies (NCOLS)*, vol. 2, no. 1, 43-60. 2020. 48-49.

⁸ Dewi, Sinta. "Konsep Perlindungan Hukum Atas Privasi Dan Data Pribadi Dikaitkan Dengan Penggunaan Cloud Computing Di Indonesia." *Yustisia Jurnal Hukum* 5, no. 1 (2016): 35-53. 35.

⁹ Dewan Perwakilan Rakyat Republik Indonesia, 2020. *Rapat Dengar Pendapat Umum (RDPU) Komisi I DPR RI dengan Pakar mengenai RUU Perlindungan Data Pribadi*, diselenggarakan pada 1 Juli 2020. 41.

¹⁰ Privacy International, 2019. "State of Privacy Indonesia". URL: <https://privacyinternational.org/state-privacy/1003/state-privacy-indonesia>. Diakses 19 April 2022.

Advokat Komang Darmayasa, S.H, M.H. dari kantor hukum DYS Law Firm menjelaskan advokasi terhadap korban pencurian data pribadi (*identity theft*) bisa dilakukan dalam ranah pidana, perdata, dan administratif¹¹. Korban yang data pribadinya dicuri dapat membuat laporan tindak pidana ke kepolisian setempat dengan dugaan tindak pidana pencurian sebagaimana dalam Pasal 362 Kitab Undang-Undang Hukum Pidana (KUHP)¹². Pelaku pencurian juga dapat dilaporkan atas dugaan pengaksesan komputer dan/atau sistem komputer secara ilegal berdasarkan Pasal 30 ayat (2) UU ITE dan dapat dikenakan ancaman sanksi pidana berupa pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp700.000.000,00 (tujuh ratus juta rupiah) didasarkan atas Pasal 46 ayat (2) UU ITE. Darmayasa menuturkan belum adanya pengaturan mengenai bentuk perlindungan hukum kepada korban dalam UU ITE¹³. Pelaku tindak pidana pencurian melalui dunia siber ini seharusnya berkewajiban untuk memberikan restitusi kepada korbannya sebagai bentuk pertanggungjawabannya, besar dan jenis bentuk restitusi yang diterima korban dapat ditentukan oleh hakim dalam amar putusannya. Bentuk restitusi dapat berupa pengembalian harta kekayaan (materi).

Terkait dengan langkah perdata yang dapat diambil korban pencurian data pribadi, Darmayasa menjelaskan korban dapat melakukan gugatan perdata atas kerugian yang diderita dilandaskan atas Pasal 26 ayat (2) UU ITE oleh sebab penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan orang yang bersangkutan (*vide* Pasal 26 ayat (1) UU ITE). Pengajuan gugatan atas kerugian tersebut juga disebut dalam Pasal 32 Permenkominfo PDPSE yang diatur bahwa:

- (1) Dalam upaya penyelesaian sengketa secara musyawarah atau melalui upaya penyelesaian alternatif lainnya belum mampu menyelesaikan sengketa atas kegagalan perlindungan kerahasiaan Data Pribadi, setiap Pemilik Data Pribadi dan Penyelenggara Sistem Elektronik dapat mengajukan gugatan atas terjadinya kegagalan perlindungan rahasia Data Pribadi.
- (2) Gugatan sebagaimana dimaksud pada ayat (1) hanya berupa gugatan perdata dan diajukan sesuai dengan ketentuan peraturan perundang-undangan.

Pengajuan gugatan ganti rugi terhadap pihak yang menggunakan data pribadi tanpa izin didasarkan atas Pasal 1365 Kitab Undang-Undang Hukum Perdata

¹¹ Hasil wawancara dengan Advokat Komang Darmayasa, S.H., M.H. pada tanggal 13 April 2022

¹² Unsur mengambil seluruhnya atau sebagian kepunyaan orang lain atau kerap dipersamakan dengan unsur barang yang diambil adalah baik berupa barang berwujud maupun barang yang tidak berwujud. Awalnya barang yang dimaksud dalam Pasal 362 KUHP adalah hanya berupa barang berwujud. Namun, semenjak *Hoge Raad* memberikan putusannya tanggal 23 Mei 1921 terhadap kasus pencurian listrik, maka makna dan pemahaman terhadap istilah bertambah bukan hanya berupa barang berwujud tetapi juga barang tidak berwujud (dalam kasus *a quo*) yang masih termasuk di dalam makna 'barang' sebagaimana dimaksudkan dalam Pasal 362 KUHP (dulunya Pasal 310 N.W.v.S.). Penafsiran demikian disebut penafsiran ekstensif sebagai pembuka pemahaman yang lebih lengkap terhadap unsur yang ada di dalam aturan hukum, sehingga menutup celah ketiadaan pengaturan terhadap perkembangan zaman nantinya. Dengan begitu, data pribadi yang termasuk ke dalam "barang tidak berwujud" dapat dalam penerapannya ketika terjadi pencurian data pribadi bisa dilakukan dengan mengenakan Pasal 362 KUHP.

¹³ Hasil wawancara dengan Advokat Komang Darmayasa, S.H., M.H., *loc.cit.*

(KUHPperdata). Darmayasa menjelaskan lebih lanjut bahwa Permenkominfo PDPSE hanya memberikan sarana penyelesaian sengketa bagi setiap orang yang memperoleh, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarluaskan data pribadi tanpa hak dengan penjatuhan sanksi administratif. Pengaturan tersebut termuat dalam Pasal 36 Permenkominfo PDPSE¹⁴. Sanksi administratif yang dapat dijatuhkan kepada pelanggar berupa: a. peringatan lisan; b. peringatan tertulis; c. penghentian sementara kegiatan; dan/atau d. pengumuman di situs dalam jaringan (*website online*).

Adapun I Wayan Atmanu Wira Pratana, S.H. selaku Co-Founder LegalPartner.id berdasarkan hasil wawancara menyatakan beberapa isu privasi dan keamanan data yang sering terjadi menurut data yang dikumpulkannya dari penyebaran kuesioner kepada masyarakat dengan target sasaran usia 17 sampai dengan 33 tahun dan dengan hasil responden berjumlah 93 orang dinyatakan bahwa sebagian besar sejumlah 74 responden atau dengan nilai persentase sebesar 79,4% isu berupa difoto/direkam tanpa izin merupakan pelanggaran privasi yang paling kerap terjadi¹⁵. Kemudian diikuti dengan isu *revenge porn* (menyebarkan konten porno) dan kebocoran data pengguna aplikasi yang direspons oleh 72 responden atau dengan nilai 77,4% dan isu terakhir berupa SMS spam yang direspons oleh 29 responden atau dengan nilai 31,2%¹⁶.

Dipaparkan lebih lanjut oleh Atmanu bahwa data-data yang digolongkan sebagai "data sensitif" atau tergolong privasi dan tidak seharusnya tersebar di media sosial atau tidak seharusnya dikumpulkan oleh penyedia jasa layanan diantaranya: a) Nomor Induk Kependudukan (NIK); b) Data pribadi; c) Alamat rumah, lokasi; d) nomor telepon; e) sidik jari; f) gender; g) email; dll. Selain itu, kasus pelanggaran privasi yang sering disebut oleh responden meliputi pinjaman *online*, *revenge porn*, dan paparazi.

Umumnya aktivitas pembobolan data pribadi terjadi oleh karena ketika calon korban diminta oleh suatu layanan elektronik (penyelenggara sistem elektronik) untuk menyetujui permintaan akses data pada perangkat yang digunakan melalui *Term & Condition*, calon korban cenderung memberikan persetujuan tanpa membaca isi dari *Term & Condition* dengan nilai data 52,7%. Lebih lanjut dikatakan oleh Atmanu bahwa kecenderungan pemberian persetujuan secara asal disebabkan sebagian besar atau sejumlah 73,5% responden atau si calon korban 'terpaksa' atau tidak ada pilihan lain untuk menyetujui persyaratan agar bisa menggunakan layanan tersebut. Maka dari itu, ketika telah memberikan persetujuan, pihak penyelenggara sistem elektronik dapat memanfaatkan akses data pribadi dari pemilik data untuk kepentingannya¹⁷.

Kebocoran data pribadi yang disebabkan oleh salah pengelolaan oleh penyelenggara sistem elektronik menjadikan isu pembentukan lembaga independen pengawas pemanfaatan data perlu segera dibentuk. Dinyatakan oleh Atmanu berdasarkan data yang dihipunnya, sebanyak 58,1% responden berpendapat sangat penting untuk segera dibentuk Lembaga Independen yang bertugas sebagai pengawas pemanfaatan data yang kemudian diikuti dengan 35,5% responden menyatakan hal tersebut penting¹⁸. Lembaga ini nantinya bertugas secara khusus menangani isu

¹⁴ *Ibid.*

¹⁵ Hasil wawancara dengan I Wayan Atmanu Wira Pratana, S.H. pada 15 Juli 2022

¹⁶ *Ibid.*

¹⁷ *Ibid.*

¹⁸ *Ibid.*

keamanan data di Indonesia yang pembentukannya harus dimuat pula dalam Rancangan Undang-Undang Perlindungan Data Pribadi yang sedang digodok untuk disahkan oleh legislator dan pemerintah. Kekosongan hukum di bidang perlindungan data pribadi menjadikan bias dan celah bagi penegakan hukum kebocoran data pribadi. Walaupun telah diatur secara parsial dan sektoral, masih terdapat pula celah yang belum terjangkau dari hadirnya UU ITE sebagai fondasi penegakan hukum di bidang teknologi informasi. Senada dengan yang disampaikan oleh Advokat Komang Darmayasa, Atmanu menyampaikan pula bahwa langkah hukum ketika terjadi kebocoran data adalah dengan mengajukan gugatan perdata ke pengadilan atau dapat pula mengadukan hal tersebut kepada Kementerian Kominfo agar segera diselesaikan melalui jalur non litigasi ada penyelesaian dengan langkah administratif berupa penjatuhan sanksi kepada pihak penyelenggara sistem elektronik. Korban yang mengalami kebocoran data juga dapat mengajukan laporan kepada kepolisian agar pihak yang membobol atau menggunakan data pribadi pemilik data secara tidak patut dilakukan pengusutan secara pidana. Pihak yang dituju terhadap langkah hukum secara pidana ini ialah pihak pembobol data pribadi dan bukan penyelenggara sistem elektronik yang mengalami kegagalan perlindungan data.

Selain itu, informasi serupa juga disampaikan oleh Prof. Dr. I.B. R Supancana selaku *Co-Founder* dari Asosiasi Profesional Perlindungan Data Indonesia. Berdasarkan hasil wawancara, Supancana menyatakan bahwa isu perlindungan data pribadi sejatinya sudah dibahas sejak tahun 2020, di mana urgensi pengaturannya ini dilatarbelakangi oleh peningkatan pesat teknologi dan informasi dalam pelbagai layanan dan jasa yang ingin mengakses data pribadi dan menggunakannya sebagai basis layanan. Data yang dikutip dari Asosiasi Pengguna Jasa Internet Indonesia (APJII) Tahun 2022 menyatakan bahwa 210.026.769 jiwa dari total populasi 272.682.600 jiwa penduduk Indonesia Tahun 2021 atau sejumlah 77,02% masyarakat Indonesia telah terkoneksi internet¹⁹.

Alasan responden menggunakan internet dijabarkan dalam data tersebut adalah sebesar 98,02% menyatakan penggunaan internet untuk dapat mengakses sosial media (termasuk Facebook/Whatsapp/Telegram/Line/Twitter/Instagram/Youtube/dll), mengakses berita atau informasi sebesar 92,21%, dan terbesar ketiga adalah untuk dapat melakukan bekerja atau bersekolah dari rumah sejumlah 90,21%²⁰.

Supancana menuturkan bahwa dengan jumlah pengguna internet khususnya pada penyedia jasa layanan tersebut yang begitu besar, potensi pembobolan data pribadi serta data yang bersifat kredensial akan semakin besar pula. RUU PDP yang saat ini sedang dibahas oleh legislator perlu segera disahkan mengingat jaminan perlindungan data pribadi merupakan segenap pemenuhan hak asasi manusia²¹.

Supancana menambahkan, apabila terjadi kebocoran data pribadi, menurut pilihan hukum yang tersedia saat ini dengan berdasar pada UU ITE beserta aturan turunannya, langkah hukum yang sebaiknya ditempuh ketika mengalami pembobolan data pribadi adalah dengan melihat permasalahan hukum yang dihadapi²². Apabila

¹⁹ Asosiasi Penyelenggara Jasa Internet, 2022. "Hasil Survei Profil Internet Indonesia 2022." URL: <https://apjii.or.id/content/read/39/559/Laporan-Survei-Profil-Internet-Indonesia-2022>. Diakses pada 14 Juni 2022.

²⁰ *Ibid.*

²¹ Hasil wawancara dengan Prof. Dr. I.B. R Supancana pada 10 Juli 2022

²² *Ibid.*

korban pembobolan data pribadi merasa dirugikan secara materiil, korban dapat membuat gugatan ganti rugi kepada pihak yang menyediakan jasa layanan yang telah gagal melindungi data pribadi si korban sehingga terjadi kebocoran dan penyalahgunaan data. Sejalan dengan langkah hukum perdata tadi, korban dapat sekaligus melaporkan kasus kebocoran data pribadi ini kepada pihak kepolisian yang nantinya akan menangani dalam ranah pidana. Pihak kepolisian nantinya dapat menggunakan UU ITE sebagai payung hukum dalam penanganan kegagalan perlindungan data pribadi. Disamping itu, korban pun dapat mengadukan permasalahan hukum yang dihadapi kepada Kemenkominfo. Melalui Kominfo, korban dapat dimediasi kepada pihak penyedia jasa layanan yang melakukan kegagalan perlindungan data pribadi atau Kominfo dapat menjatuhkan sanksi administratif atas kegagalan yang dimaksud²³.

Secara garis besar, korban yang mengalami kebocoran data pribadi dapat menempuh langkah melalui:

1. Jalur Litigasi

Jalur litigasi yang dapat ditempuh oleh korban dapat berupa penyelesaian perkara dalam ranah pidana atau perdata dengan sama-sama bermuara pada putusan pengadilan. Jika korban menempuh langkah hukum pidana, pihak yang dilaporkan kepada kepolisian adalah pihak yang membobol dan menyalahgunakan data pribadi korban. Penyelesaian perkara secara pidana dimulai dengan melaporkan kasus kebocoran data pribadi kepada pihak kepolisian setempat atas dugaan pencurian data sebagaimana Pasal 362 KUHP atau dugaan pengaksesan komputer dan/atau sistem komputer secara ilegal berdasarkan Pasal 30 ayat (2) UU ITE. Lain halnya jika korban ingin menuntut ganti kerugian secara keperdataan atas terjadinya kegagalan perlindungan data pribadi, maka pihak yang diperkarakan *casu quo* adalah penyelenggara sistem elektronik dengan cara mengajukan gugatan perdata ke pengadilan negeri sebagaimana gugatan ganti rugi dalam Pasal 1365 KUHP perdata.

2. Jalur Non Litigasi

Jalur non litigasi menjadi pilihan bagi korban yang tidak ingin menempuh penyelesaian perkara melalui pengadilan. Pilihan jalur non litigasi yang disediakan Permenkominfo PDPSE adalah dengan mengadukan perkara kebocoran data kepada Menteri yang menyelenggarakan urusan pemerintahan di bidang komunikasi dan informatika. Menteri terkait mempunyai pilihan dalam menyelesaikan perkara dengan menjatuhkan sanksi administratif kepada penyelenggara sistem elektronik atau mempertemukan korban dengan pihak penyelenggara sistem elektronik untuk mencari solusi terbaik atas permasalahan yang dihadapi.

4. Kesimpulan

Terhadap pembahasan yang telah disajikan sebelumnya, dapat ditarik suatu kesimpulan bahwawa Kewajiban Pemerintah Negara Indonesia dalam memberikan perlindungan data pribadi didasarkan pada ketentuan pada Pasal 28G ayat (1) UUD NRI Tahun 1945. Kewajiban pemerintah tersebut kemudian diderivikasikan melalui beberapa peraturan perundang-undangan di Indonesia. Namun, beberapa peraturan tersebut belum memberikan pengaturan mengenai perlindungan hukum secara umum bagi korban yang data pribadinya bocor. Selain itu, langkah konkret yang dapat diambil oleh korban ketika datanya bocor adalah dengan pengajuan perkara secara

²³ *Ibid.*

litigasi atau non litigasi. Secara litigasi, perkara dapat dibuatkan laporan kepolisian sehingga akan diusut sebagai perkara pidana. Namun, jika korban ingin menuntut kerugian, penyelesaian dapat dilakukan dengan mengajukan gugatan perdata ganti rugi ke pengadilan terhadap pihak penyelenggara sistem elektronik atas kegagalan perlindungan data pribadi. Apabila perkara ingin diselesaikan melalui jalur non litigasi, korban dapat mengadukan perkara tersebut kepada Menteri yang menyelenggarakan urusan pemerintahan di bidang komunikasi dan informatika. Langkah yang akan diambil oleh Menteri adalah dengan mempertemukan korban dengan pihak penyelenggara sistem elektronik untuk mencari solusi terbaik atau Menteri dapat menjatuhkan sanksi secara administratif. Adapun saran yang dapat diberikan dalam studi ini ialah Para korban yang merasa dirugikan haknya dapat menyelesaikan perkara kebocoran data pribadinya ke pengadilan sebagai perwujudan asas *ius curia novit*, karena bila pun terjadi kekosongan norma, berdasarkan asas tersebut hakim dianggap tahu hukum dan harus mencari hukumnya sebagai jawaban atas kekosongan norma tersebut. Selain itu, kepada pembentuk undang-undang hendaknya segera mengesahkan rancangan undang-undang mengenai perlindungan data pribadi untuk mengisi kekosongan hukum dan menjamin kepastian hukumnya

DAFTAR PUSTAKA

Buku:

Karo, Rizky P.P. Karo, *Pengaturan Perlindungan Data Pribadi di Indonesia: Perspektif Teori Keadilan Bermartabat*, Nusa Media, Jakarta, (2020)

Jurnal Ilmiah:

Ayu D., Ananthia, Titis Anindyajati, dan Abdul Ghoffar, 2019. "Perlindungan Hak Privasi atas Data Diri di Era Ekonomi Digital". *Hasil Penelitian*. Kepaniteraan dan Sekretariat Jenderal Mahkamah Konstitusi.

Ewi, Sinta. "Konsep Perlindungan Hukum Atas Privasi Dan Data Pribadi Dikaitkan Dengan Penggunaan Cloud Computing Di Indonesia." *Yustisia Jurnal Hukum* 5, no. 1 (2016)

Fathur, Muhammad. "Tanggung Jawab Tokopedia Terhadap Kebocoran Data Pribadi Konsumen." In *National Conference on Law Studies (NCOLS)*, vol. 2, no. 1, (2020)

Sautunnida, Lia. "Urgensi Undang-Undang Perlindungan Data Pribadi di Indonesia: Studi Perbandingan Hukum Inggris dan Malaysia." *Kanun Jurnal Ilmu Hukum* 20, no. 2 (2018)

Situmeang, Sahat Maruli Tua. Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna dalam Perspektif Hukum Siber. *Jurnal SASI Volume 27 Nomor 1* (2019): 38-52. DOI: 10.47268/sasi.v27i1.394

Wulansari, e.m., "Kosep Perlindungan Data Pribadi Sebagai Aspek Fundamental Normdalam Perlindungan Terhadap Hak Atas Privasi Seseorang di Indonesia." *Jurnal Surya Kencana Dua: dinamika masalah hukum dan keadilan*, 20, no.2 (2018)

Yuniarti, S., "Perlindungan hukum data pribadi di Indonesia. *Business Economic, Communication, and Social Sciences (BECOSS) Journal*," 1, no.1 (2019)

Internet:

Asosiasi Penyelenggara Jasa Internet, 2022. "Hasil Survei Profil Internet Indonesia 2022." URL: <https://apjii.or.id/content/read/39/559/Laporan-Survei-Profil-Internet-Indonesia-2022>. Diakses pada 14 Juni 2022.

Privacy International, 2019. "State of Privacy Indonesia". URL: <https://privacyinternational.org/state-privacy/1003/state-privacy-indonesia>. Diakses pada 19 April 2022.

Reza Hadyan, 2021, "Tagihan Palsu dan Rentannya Penyalahgunaan Data Pribadi", URL: <https://teknologi.bisnis.com/read/20210425/84/1385873/tagihan-palsu-dan-rentannya-penyalahgunaan-data-pribadi>, diakses pada 15 Desember 2021, Pukul 17.50 WITA.

Peraturan Perundang-Undangan

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945

Kitab Undang-Undang Hukum Perdata (KUHPerdata)

Kitab Undang-Undang Hukum Pidana (KUHP)

Undang-Undang Nomor 17 Tahun 2007 tentang Rencana Pembangunan Jangka Panjang 2005-2025

Undang-Undang Nomor 24 Tahun 2013 tentang Perubahan atas Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan

Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi

Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem Dan Transaksi Elektronik