



PERLINDUNGAN HUKUM KONSUMEN TERHADAP *IDENTITY THEFT* MENURUT UNDANG-UNDANG NOMOR 27 TAHUN 2022

Oleh

Randy Ireneus Hendrik, Chinelsya Rimanitha Tappangrara, Anastasia Eveline Langa

Perlindungan Hukum Konsumen Terhadap *Identity Theft* Menurut Undang-Undang

Nomor 27 Tahun 2022

Oleh:

Randy Ireneus Hendrik, Chinelsya Rimanitha Tappangrara, Anastasia Eveline Langa

BAB I

PENDAHULUAN

A. Latar Belakang

Indonesia adalah negara hukum sebagaimana diatur dan diamanatkan dalam Pasal 1 ayat (3) UUD NRI 1945. Namun dalam prosesnya, terkadang hukum yang berlaku tidak diimplementasikan dengan baik, salah satunya regulasi yang berhubungan perlindungan data pribadi.¹ Hadirnya teknologi mendorong perubahan sistem perekonomian masyarakat, yang awalnya bersifat tradisional berbasis manufaktur, berubah menjadi ekonomi digital. Namun, perkembangan teknologi juga membawa dampak negatif, salah satunya ancaman kebocoran data pribadi penggunanya. Berdasarkan data yang dilaporkan oleh Kementerian Komunikasi dan Informasi pada siaran pers yang dilakukan pada 5 Juli 2023, diketahui bahwa telah terjadi kebocoran data pribadi penduduk Indonesia sebanyak 34.900.867.²

Dalam konstitusi, perlindungan data pribadi³ seseorang dapat kita temukan dalam Pasal 28D ayat (1) UUD NRI 1945, yang mengamanatkan bahwa setiap orang berhak untuk mendapatkan perlindungan dari negara. Dalam hal ini, mencakup perlindungan atas data pribadi yang tergolong ke dalam hak asasi setiap orang sebagaimana diatur lebih lanjut dalam Pasal 28G ayat (1).⁴ Penegasan terkait dengan perlindungan data pribadi sebagai bentuk perlindungan terhadap hak asasi, dapat kita lihat dalam Pasal 29 Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia. Mengingat urgensi perlindungan data pribadi menjadi salah satu poin yang diamanatkan oleh konstitusi,

¹ Pasal 1 Angka 1 Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

² Biro Humas Kementerian Kominfo 'Telusuri Dugaan Kebocoran Data Paspor 34Juta Warga Indonesia' (Kominfo, 2023) https://www.kominfo.go.id/content/detail/50017/siaran-pers-no-132hmkominfo072023-tentang-kominfo-telusuri-dugaan-kebocoran-data-paspor-34-juta-warga-indonesia/0/siaran_pers diakses pada 24 September 2023.

³ Pasal 1 Angka 3 Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

⁴ Pasal 28G ayat (1) Undang-Undang Dasar Negara Republik Indonesia tahun 1945

maka pemerintah membuat sedikitnya 30 regulasi yang mengatur hal tersebut.⁵ Namun faktanya, masih terjadi kasus kebocoran data di Indonesia, salah satunya pernah terjadi di tahun 2019, dimana kebocoran data tersebut melibatkan pihak Bukalapak dengan total 13 juta akun yang bocor.⁶

Konsep *e-commerce* yang efisien menjadi daya tarik oleh masyarakat dalam melakukan transaksi *e-commerce* dalam pemenuhan kebutuhan sehari-harinya. Kejahatan yang biasanya terjadi pada transaksi *e-commerce*, salah satunya pencurian data pribadi (*identity theft*) konsumen *e-commerce* untuk dijual kepada pihak tertentu. Hal ini dapat terjadi karena karena dalam melakukan kegiatan transaksi *e-commerce*, terlebih dahulu penyelenggara sistem elektronik melakukan pengelolaan data-data pribadi para pengguna seperti dengan meminta identitas berupa nama, tempat tinggal lahir, jenis kelamin, alamat tempat tinggal, alamat email, kotak pribadi bahkan tidak jarang meminta scan KTP konsumen.⁷

Kejahatan transaksi *e-commerce* kerap disebut dengan kejahatan siber (*cyber crime*), dimana bentuk kejahatan yang dilakukan dengan menggunakan teknologi komputer dan/atau jaringan komputer untuk menguntungkan diri sendiri atau orang lain dan merugikan pihak lain.⁸ Kebocoran data pribadi dalam transaksi *e-commerce* di Indonesia dapat terjadi karena 3 (tiga) faktor utama yaitu Standar Operasional Prosedur (SOP), Sumber Daya Manusia (SDM) dan Teknologi.⁹ Salah satu dampak transaksi *e-commerce* adalah *identity theft*.

Menurut Black's Law Dictionary, *identity theft* adalah perbuatan yang dengan sengaja memperoleh atau mengambil informasi pribadi orang lain untuk tujuan kriminal. Berbeda dengan pembobolan data (data breach), *identity theft* tidak harus membobol sistem keamanan tempat data pribadi diamankan. Indonesia memiliki pengaturan data

⁵ Wahyudi Djafar, Bernhard Ruben Fritz Sumigar, Blandina Lintang Setianti, *Perlindungan Data Pribadi: Usulan Pelembagaan Kebijakan dari Perspektif Hak Asasi Manusia*, (Lembaga Studi dan Advokasi Masyarakat: ELSAM 2016). [62].

⁶ Indiana Malia 'Sebelum BPJS Kesehatan, Ini 3 Kasus Kebocoran Data Konsumen *E-commerce*' (IDN Times, 2021) <https://www.idntimes.com/business/economy/indianamalia/selain-bpjjs-kesehatan-ini-3-kasus-kebocoran-data-konsumen-e-commerce> diakses pada 29 September 2023.

⁷ Gillang Achmad Riyadi, Toto Tohir Suriaatmadja, 'Perlindungan Hukum atas Kebocoran Data Pribadi Konsumen PT PLN Dihubungkan dengan Hak Atas Keamanan Pribadi Ditinjau dari Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi' Bandung Conference Series (Law Studies IV 2023). [228].

⁸ Ida Kurnia, Imelda Martinelli, 'Permasalahan Dalam Transaksi *E-Commerce*' (2021) IV Jurnal Bakti Masyarakat Indonesia. [334].

⁹ T. Rahmat Kautsar, 'Kajian Literatur Terstruktur Terhadap Kebocoran Data Pribadi dan Regulasi Perlindungan Data Pribadi', (Skripsi, Universitas Islam Negeri Ar-Raniry 2023). [27].

pribadi dalam sistem perundang-undangan, seperti Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang- Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), Peraturan Menteri Komunikasi dan informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem elektronik (Perkominfo PDPSE), dan Peraturan Pemerintah Nomor 71 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE). Namun, aturan-aturan tersebut masih memiliki kelemahan sebagaimana yang akan dijelaskan dalam pembahasan. Sebagai upaya peningkatan keamanan data pribadi masyarakat, Indonesia mengundangkan UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi yang mengacu pada substansi General Data Protection Regulation (GDPR).

B. Rumusan Masalah

Adapun rumusan masalah dalam tulisan ini adalah:

1. Bagaimana bentuk perlindungan hukum konsumen terhadap identity theft dalam transaksi *e-commerce* menurut UU PDP?
2. Apakah regulasi yang ada saat ini di Indonesia mampu memberikan perlindungan hukum bagi konsumen *e-commerce* terhadap Identity Theft menurut UU PDP?

BAB II

PEMBAHASAN

A. Perlindungan Hukum Konsumen Terhadap *Identity Theft* dalam Transaksi *E-Commerce* Menurut Undang-Undang Perlindungan Data Pribadi.

Di Indonesia, perlindungan konsumen telah diatur dalam Undang- Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen (UU PK). Pasal 1 angka 1 menerangkan bahwa Perlindungan konsumen adalah segala upaya yang menjamin adanya kepastian hukum untuk memberi perlindungan kepada konsumen.¹⁰ UU PK hadir untuk menjamin perlindungan konsumen dan pelaku usaha dalam hubungan interaksi jual beli.

Upaya preventif Pasal 28 huruf C Perkominfo PDPSE, tidak efektif dalam mencegah penyalahgunaan data pribadi yang bocor atau dicuri. Mengingat pemberitahuan bisa saja telat atau tidak langsung diketahui oleh Pemilik Data Pribadi. Untuk itu, sangat perlu pembentukan suatu lembaga yang ditunjuk oleh undang-undang dalam bertanggung jawab dalam mencegah data pribadi yang bocor lalu dicuri oleh oknum yang tidak bertanggung jawab.

Dalam Pasal 32 UU ITE telah diatur sanksi pidana yang berkaitan dengan *identity theft*. Namun, pasal tersebut tidak cukup untuk mendefinisikan tindakan *identity theft* secara sempit. Selain itu, UU ITE belum mengatur secara kuat mengenai pertanggungjawaban *e-commerce* sebagai penyelenggara sistem elektronik dalam melindungi konsumen dari tindakan *identity theft* dan pengaturan sanksi yang dapat dibebankan kepada pegawai *e-commerce* atas kelalaian dalam menjaga data pribadi. Adapun peraturan turunan UU ITE, yaitu PP PSTE, telah mengatur prinsip-prinsip perlindungan data pribadi dan cakupan pemrosesan data pribadi. Namun, PP PSTE tidak memiliki ketentuan teknis pemrosesan data pribadi dan hanya memiliki sanksi administratif.

Berdasarkan kelemahan-kelemahan regulasi yang telah dipaparkan di atas, UU PDP diharapkan mampu menjadi harapan baru untuk melindungi data pribadi konsumen dari *identity theft* dalam transaksi *e-commerce*. Sejalan dengan perlindungan hukum, Philipus M. Hadjon menjelaskan bahwa perlindungan hukum terbagi dua yaitu perlindungan hukum preventif sebagai upaya pencegahan terjadinya sengketa dan

¹⁰ Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen.

perlindungan hukum represif sebagai upaya penyelesaian sengketa.¹¹ Adanya perlindungan hukum dapat menjelaskan bahwa fungsi hukum telah bekerja untuk memberikan keadilan, kemanfaatan, dan kepastian hukum.¹²

1. Upaya Preventif

Untuk memastikan setiap *e-commerce* memiliki standar keamanan yang dapat dipercaya oleh konsumen, UU PDP melalui Pasal 20 ayat (1) mewajibkan setiap *e-commerce* memiliki dasar pemrosesan yang sah. Dalam *e-commerce*, dasar pemrosesan data pribadi dapat dijumpai dalam kebijakan privasi. Dasar tersebut menjadi dasar perjanjian pemrosesan data pribadi antara *e-commerce* dan konsumen sebagai upaya penjaminan keseimbangan hak dan kewajiban para pihak. Dasar tersebut nantinya akan menjelaskan batasan tanggung jawab suatu *e-commerce* apabila terjadi kebocoran data pribadi. Agar dasar tersebut dapat dianggap sah, ia harus memenuhi ketentuan-ketentuan yang diatur dalam Pasal 20 ayat (2) sampai Pasal 26.

Untuk mencegah terjadinya kebocoran data pribadi, UU PDP mengatur kewajiban-kewajiban pengendali data pribadi dan prosesor data pribadi dalam Pasal 27-54. Ketentuan-ketentuan tersebut mewajibkan setiap *e-commerce* untuk memiliki tingkat keamanan privasi yang tinggi dan merencanakan metode pemrosesan data pribadi sesuai ketentuan UU PDP sebelum dan saat pemrosesan dilakukan. Upaya tersebut sesuai dengan prinsip *protection by design* menurut Pasal 25 GDPR. Agar prinsip tersebut dapat sepenuhnya terpenuhi, perlindungan data pribadi harus diamankan menggunakan desain teknologi yang andal. Contoh teknologi yang penting untuk digunakan dalam melindungi data pribadi adalah *Data Loss Prevention*, *firewalls*, enkripsi, pemetaan data, dan *endpoint protection*.¹³

Untuk mencegah terjadinya kelalaian pemrosesan data pribadi oleh pihak *e-commerce*, Pasal 53 UU PDP mewajibkan setiap *e-commerce* menunjuk pejabat atau petugas pelaksana fungsi Pelindungan Data Pribadi

¹¹ Winsherly Tan, ‘Problematika Perkawinan di Bawah Umur dan Tantangan dalam Mencapai Sustainable Development Goals (SDGs)’ (2021) VII JUSTISI 7. [81-82].

¹² Zaenal Arifin dan Muhammad Iqbal, ‘Perlindungan Hukum terhadap Merek yang Terdaftar’ (2020) V Jurnal Ius Constituendum 5. [60]

¹³ Dewi Sulistianingsih, dkk, ‘Tata Kelola Perlindungan Data Pribadi di Era Metaverse (Telaah Yuridis Undang-Undang Perlindungan Data Pribadi)’ (2023) LII Jurnal Masalah-Masalah Hukum. [103].

yang memenuhi standar profesionalitas, pengetahuan mengenai hukum, praktik Pelindungan Data Pribadi, dan kemampuan untuk memenuhi tugas-tugasnya. Pejabat atau petugas tersebut juga disebut sebagai *Data Protection Officer* (DPO) yang dapat berasal dari dalam dan/atau luar Pengendali Data Pribadi atau Prosesor Data Pribadi.

Pemerintah melalui lembaga yang disebut dalam Pasal 58 UU PDP akan bertanggung jawab dalam menjamin terlaksananya penyelenggaraan pelindungan data pribadi dan hak konstitusional subjek data pribadi. Bentuk upaya yang dapat dilakukan lembaga tersebut adalah dengan melaksanakan wewenang-wewenangnya sesuai Pasal 60. Dari wewenang-wewenangnya itu, lembaga dapat mencegah pelaku *identity theft* atau setiap orang yang tidak berwenang menyalahgunakan data pribadi yang bocor, misalnya dengan melaksanakan ketentuan huruf i sampai huruf o.

2. Upaya Represif

Dalam UU PDP, tidak ada ketentuan yang secara eksplisit mengatur tentang kelalaian pengendali data pribadi atau prosesor data pribadi yang mengakibatkan kebocoran data pribadi. Namun, kelalaian tetap dapat dianggap sebagai suatu kesalahan karena mengabaikan kehati-hatian sehingga menyebabkan sesuatu terjadi dengan tidak sengaja.¹⁴ Mengingat UU PDP berasaskan asas kehati-hatian dan asas pertanggungjawaban, maka pihak *e-commerce* seharusnya mampu memperhatikan segenap aspek yang berpotensi mendatangkan kerugian dan mampu bertanggung jawab apabila merugikan konsumen akibat ulahnya sendiri. Sehingga jika kebocoran data pribadi terjadi akibat kelalaian pihak *e-commerce*, maka seharusnya ia tetap dapat dimintakan pertanggungjawaban, sebagaimana diatur oleh Pasal 12.

Walaupun tidak ada ketentuan pidana atau sanksi administratif terkait kelalaian dalam UU PDP, dampak dari kelalaian seperti kebocoran data pribadi dapat mengindikasikan terjadinya kegagalan perlindungan data pribadi¹⁵ sebagaimana disebut dalam Pasal 46. Kegagalan perlindungan data pribadi tersebut dapat timbul akibat pelanggaran terhadap kewajiban-

¹⁴ Tofik Yanuar Chandra, *Hukum Pidana* (Sanggr Multi Usaha 2022). [77].

¹⁵ Pasal 46 ayat (1) Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.

kewajiban pengendali data pribadi atau prosesor data pribadi. Apabila demikian, maka hal tersebut memenuhi ketentuan Pasal 57 yang memiliki sanksi administratif.

Untuk pelaku *identity theft* dapat diberat sanksi pidana jika secara kumulatif memenuhi unsur-unsur Pasal 67 ayat (1). Artinya, pelaku *identity theft* harus dilakukan oleh orang perseorangan atau korporasi. Ia harus dengan sengaja memperoleh atau mengumpulkan data pribadi yang bukan miliknya, padahal ia tidak memiliki dasar pemrosesan data pribadi yang sah. Ia memiliki niat untuk menguntungkan diri sendiri atau orang lain dan atas perbuatannya itu berpotensi dan/atau langsung merugikan subjek data pribadi.

Jika ketentuan pidana UU PDP dilakukan oleh korporasi, maka ketentuan sanksi pidananya merujuk Pasal 70. Artinya, sanksi pidana Pasal 60 ayat (1) dapat dijatuhan kepada pengurus, pemegang kendali, pemberi perintah, pemilik manfaat, dan/atau korporasi apabila tindakan *identity theft* dilakukan oleh sesama pihak *e-commerce*. Sedangkan sanksi pidana korporasi hanya dapat dijatuhan pidana denda dan pidana tambahan menurut ayat (4). Apabila harta kekayaan atau pendapatan korporasi yang disita tidak cukup untuk melunasi pidana denda, maka korporasi dikenakan pidana pengganti berupa pembekuan sebagian atau seluruh kegiatan usaha korporasi untuk jangka waktu paling lama 5 (lima) tahun.

B. Perlindungan Hukum Bagi Konsumen *E-Commerce* Terhadap *Identity Theft* Menurut Undang-Undang Perlindungan Data Pribadi.

Jika di cermati secara seksama masih terdapat beberapa kekurangan dalam UU PDP. Pasal 51 ayat (3) UU PDP hanya mengatur bahwa pengendali data pribadi bertanggungjawab atas pemrosesan data. Akan tetapi, tidak ada penjelasan secara eksplisit mengenai apa saja bentuk pertanggungjawaban yang dapat dilakukan oleh pengendali data. Jika didasarkan pada keberlakuan asas *actori incumbit probatio*, ketidakjelasan konsep pertanggungjawaban ini akan menimbulkan permasalahan baru dalam hal pengajuan gugatan ganti kerugian. Kedudukan subjek data pribadi yang lebih rendah dibandingkan pihak yang melakukan penyalahgunaan data pribadi. Sehingga jika dikaitkan dengan asas tersebut, sangatlah sulit bagi subjek data pribadi untuk memberikan

pembuktian, terlebih jika subjek data pribadi tersebut awam terhadap teknologi.

Kemudian, Pasal 56 ayat (1) menjelaskan bahwa pengendali data pribadi dapat melakukan transfer data kepada pengendali di luar wilayah hukum Negara Republik Indonesia. Akan tetapi yang menjadi permasalahan adalah dalam pasal ini tidak dijelaskan bahwa segala tindakan tersebut harus tetap didasarkan pada persetujuan pemilik data tersebut. Meskipun dalam UU PDP mengharuskan Pengendali Data Pribadi memastikan tingkat perlindungan data pribadi negara penerima transfer data tersebut setara atau lebih tinggi dari Indonesia, tetapi upaya tersebut tidak cukup mengingat kedudukan data pribadi menjadi salah satu aspek perlindungan HAM, maka pemberitahuan dan persetujuan pemilik data tetap diperlukan. Hal ini sebagaimana diatur dalam Pasal 5 UU PDP, bahwa subjek data pribadi berhak menerima informasi terkait dengan pemrosesan datamiliknya. Sehingga jika Pasal 56 ayat (1) UU PDP tidak didasarkan pada persetujuan pemilik data, maka hal tersebut bertentangan dengan pengimplementasian hak absolute rights sebagai dasar dibentuknya UU PDP itu sendiri.

Selanjutnya, melalui Pasal 58 ayat (2) dan (3) UU PDP mengamanatkan agar dibentuk satu lembaga yang bertugas untuk menyelenggarakan perlindungan data pribadi sesuai dengan ketentuan UU PDP, di mana lembaga tersebut ditunjuk oleh Presiden. Namun sayangnya, sampai saat ini belum ada lembaga yang ditunjuk untuk menjalankan penyelenggaraan perlindungan data pribadi sebagaimana telah diatur dalam UU PDP. Ketentuan mengenai lembaga perlindungan data pribadi diatur lebih lanjut di Pasal 59 huruf c UU PDP, yang menjelaskan bahwa Lembaga tersebut hanya melaksanakan penegakan hukum secara administrasi saja. Sementara UU PDP tidak hanya mengatur sanksi administrasi, tetapi juga mengatur sanksi pidana dan perdata.

Selain itu, dalam hal tata cara pengenaan sanksi administrasi sebagaimana diatur dalam Pasal 57 ayat (5) akan diatur oleh peraturan pemerintah. Namun hingga undang-undang ini berlaku, belum ada Peraturan Pemerintah yang dikeluarkan untuk mengatur mengenai hal tersebut. Penulis berpendapat bahwa ketidakjelasan pasal ini dalam mengatur kapan seseorang akan dikenakan sanksi peringatan secara tertulis, penghentian pemrosesan data, penghapusan dan pemusnahan data, hingga denda administrasi, dapat menjadi pasal karet jika tidak segera dijelaskan dan diatur dalam peraturan pemerintah mengenai tata cara pengenaannya.

Dalam UU PDP, tidak ada pasal yang mengatur atau memberikan penjelasan

mengenai sanksi mana yang akan diterapkan terlebih dahulu jika terjadi kebocoran data. Apakah kedudukan sanksi administrasi dan sanksi perdata harus didahulukan dibanding sanksi pidana atau sebaliknya. Selanjutnya, UU PDP tidak mengatur kewajiban agar seluruh pihak yang melakukan pengumpulan serta pengolahan data, wajib memiliki kemampuan yang spesifik di bidang tersebut.

Berdasarkan kelemahan-kelemahan dari UU PDP yang telah dipaparkan di atas, Penulis berpendapat bahwa hadirnya UU PDP belum mampu memberikan jaminan kepastian hukum bagi seluruh pengguna layanan *e-commerce* dari tindakan *identity theft*. Sehingga diperlukan pemberian dalam klausul-klausul pasal yang bersifat multiafsir dan mampu memberikan celah bagi oknum yang tidak bertanggung jawab melakukan penyalahgunaan data pribadi orang lain.

BAB III

PENUTUP

A. Kesimpulan

Kedudukan data pribadi sebagai salah satu aspek yang dijamin dalam Hak Asasi Manusia mendorong pemerintah untuk merangkan produk-produk hukum yang relevan. Dalam menghadapi ancaman *identity theft*, Indonesia memiliki beberapa regulasi data pribadi konsumen dalam *e-commerce*. UU PK yang berlaku di Indonesia tidak mengatur mengenai perlindungan data pribadi dalam transaksi *e-commerce*. Perkominfo PDPSE juga belum mengatur sanksi terhadap *identity theft* dan belum memiliki ketentuan yang efektif untuk mencegah penyalahgunaan data pribadi yang bocor atau dicuri. Adapun UU ITE belum mendefinisikan unsur pidana *identity theft* secara sempit, pertanggungjawaban *e-commerce* dalam melindungi konsumen dari tindakan *identity theft*, pengaturan sanksi yang dapat dibebankan kepada pegawai *e-commerce* atas kelalaian dalam menjaga data pribadi. Sedangkan, PP PTSE belum memiliki ketentuan teknis pemrosesan data pribadi dan hanya memiliki sanksi administratif. Sehingga kehadiran UU PDP, diharapkan mampu memberikan jaminan kepastian hukum bagi perlindungan data pribadi. Namun pada kenyataannya, UU PDP masih memiliki banyak kekurangan dan kelemahan. Hal ini mengakibatkan beberapa pasal yang diatur dalam UU PDP, tidak lagi berperan melindungi, tetapi juga menjadi buah simalakama bagi subjek data pribadi.

B. Saran

Dari kesimpulan tersebut, Penulis ingin menyampaikan beberapa saran bagi pelaksanaan perlindungan data pribadi di Indonesia. Adapun beberapa saran sebagai berikut:

1. Melengkapi aturan turunan dari UU PDP serta memperjelas beberapa ketentuan yang ada dalam UU PDP, seperti konsep pertanggungjawaban, agar tidak terjadi kekosongan hukum dalam proses pengimplementasiannya.
2. Demi mencegah terjadinya kebocoran data pribadi karena sistem, setiap Pengelola Data Pribadi diwajibkan untuk selalu melakukan upgrade terhadap sistem pengelolaan data dan melakukan pelaporan kepada lembaga pelindungan data pribadi setiap enam bulan sekali atau satu tahun sekali.

LEGAL REVIEW | 2023 EDITION

3. Melakukan perubahan terhadap sistem pengumpulan data, yang awalnya *single identity*, menjadi *multi identity*.

DAFTAR PUSTAKA

PERUNDANG-UNDANGAN

Undang-Undang Dasar Negara Republik Indonesia tahun 1945.

Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen.

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

JURNAL

Dewi Sulistianingsih, dkk, “Tata Kelola Perlindungan Data Pribadi di Era Metaverse (Telaah Yuridis Undang-Undang Perlindungan Data Pribadi)”, (2023), LII Jurnal Masalah-Masalah Hukum.

Ida Kurnia, Imelda Martinelli, “Permasalahan Dalam Transaksi *E-Commerce*”, (2021), IV Jurnal Bakti Masyarakat Indonesia.

Winsherly Tan, “Problematika Perkawinan di Bawah Umur dan Tantangan dalam Mencapai Sustainable Development Goals (SDGs)”, (2021), VII JUSTISI.

Zaenal Arifin dan Muhammad Iqbal, “Perlindungan Hukum terhadap Merek yang Terdaftar”, (2020) V Jurnal Ius Constituendum.

BUKU

Wahyudi Djafar, Bernhard Ruben Fritz Sumigar, Blandina Lintang Setianti, *Perlindungan Data Pribadi: Usulan Pelembagaan Kebijakan dari Perspektif Hak Asasi Manusia*, (Lembaga Studi dan Advokasi Masyarakat: ELSAM) (2016)

ARTIKEL ONLINE

Gillang Achmad Riyadi, Toto Tohir Suriaatmadja. “Perlindungan Hukum atas Kebocoran Data Pribadi Konsumen PT PLN Dihubungkan dengan Hak Atas Keamanan Pribadi Ditinjau dari Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi”

<<https://proceedings.unisba.ac.id/index.php/BCSLS/article/view/4945/2904>> diakses
25 September 2023

Biro Humas Kementerian Kominfo, “Telusuri Dugaan Kebocoran Data Paspor 34 Juta Warga Indonesia” <https://www.kominfo.go.id/content/detail/50017/siaran-pers-no-132hmkominfo072023-tentang-kominfo-telusuri-dugaan-kebocoran-data-paspor-34-juta-warga-indonesia/0/siaran_pers> diakses pada 24 September 2023.

Indiana Malia, “Sebelum BPJS Kesehatan, Ini 3 Kasus Kebocoran Data Konsumen E-Commerce” <<https://www.idntimes.com/business/economy/indianamalia/selain-bpjks-kesehatan-ini-3-kasus-kebocoran-data-konsumen-e-commerce>> diakses pada 29 September 2023.

T. Rahmat Kautsar, “Kajian Literatur Terstruktur Terhadap Kebocoran Data Pribadi dan Regulasi Perlindungan Data Pribadi” <<https://repository.araniry.ac.id/id/eprint/25647/>> diakses pada 29 September 2023.