LAW DEVELOPMENT DIVISION
2022-2023

LEGAL ARGUMENT

Volume 03 No. 4

Perlindungan Hukum Terhadap Kebocoran Data Pribadi
(Personal Data Leak)
(Studi Kasus: Dugaan Kebocoran Data 34 Juta Paspor Warga Negara Indonesia)

Author:
1. Ni Putu Sindy Indradewi Pradnyandari Putri K.
2. I Putu Gede Putra Sentana
3. Firmansyah Krisna Maulana

Reviewed by: Bima Kumara Dwi Atmaja, S.H., M.H.

Pelindungan Hukum Terhadap Kebocoran Data Pribadi *(Personal Data Leak)*

(Studi Kasus: Dugaan Kebocoran Data 34 Juta Paspor Warga Negara Indonesia)

Ni Putu Sindy Indradewi Pradnyandari Putri K., I Putu Gede Putra Sentana,

Firmansyah Krisna Maulana

I. FAKTA

Berdasarkan data yang terdapat pada CNN Indonesia, sejak 1 Januari 2023 hingga 6 Juli 2023 tercatat ada 35 dugaan kasus kebocoran data (*data leak)*[1]. Beberapa kasus besar terkait dugaan kebocoran data seperti dugaan kebocoran 100.000 sampel data pelanggan BPJS Ketenagakerjaan Indonesia pada 12 Maret 2023, dugaan pencurian 1,5 *terabyte* (TB) data pribadi nasabah Bank Syariah Indonesia (BSI) pada 8 Mei 2023, dan dugaan kebocoran 10.050 sampel data pengguna MyIndiHome pada akhir Juni 2023. Berita mengenai dugaan kasus-kasus kebocoran data ini telah meningkatkan kekhawatiran masyarakat mengenai keamanan data pribadi yang dikelola oleh instansi pemerintahan dan pelayanan publik di Indonesia. Kondisi ini mencerminkan keamanan siber di Indonesia yang masih sangat lemah dan rentan.

Berita terbaru mengenai kasus dugaan kebocoran data terjadi di awal Juli 2023 yaitu adanya dugaan kebocoran data paspor 34 juta Warga Negara Indonesia (WNI). Data yang diduga mengalami kebocoran meliputi, nomor paspor, NIKIM (National Identiti Kartu Identitas Masyarakat yang memuat nama, alamat, nomor KTP, dan NPWP), tanggal pembuatan dan tanggal kadaluarsa paspor, tanggal lahir, jenis kelamin, hingga pemutakhiran. Terduga pelaku pada kasus kebocoran data paspor WNI adalah pemilik akun anonim bernama “Bjorka”, dimana akun tersebut membagikan 1 juta sampel data nama pengguna paspor. Bjorka mengaku memiliki 34.900.867 nama pengguna paspor yang diperjualbelikan dengan harga $10.000 USD atau sekitar Rp150.000.000,00 *(seratus lima puluh juta rupiah)*.[2]

Pada 7 Juli 2023, melalui Siaran Pers No.138/HM/KOMINFO/07/2023, Direktur Jenderal Aplikasi Informatika Kementerian Kominfo Semuel A. Pangerapan menyatakan bahwa Tim Investigasi Pelindungan Data Pribadi telah melakukan investigasi awal. Kementerian Kominfo menemukan fakta adanya kemiripan dengan data paspor. Berdasarkan detil data yang ditemukan, data-data yang bocor diduga diterbitkan sebelum terjadi perubahan peraturan paspor menjadi 10 tahun, dikarenakan terlihat masa berlakunya hanya 5 tahun. Kemudian, pada 8 Juli 2023, Dirjen Informasi dan Komunikasi Publik Kominfo Usman Kansong dalam *interview*-nya dengan iNews ROOM menyebutkan bahwa telah didapatkan bukti sementara mengenai adanya kebocoran pada data paspor tahun 2020. Hal tersebut, diduga terjadi ketika proses migrasi data dari penyimpanan di Imigrasi ke PDN (Pusat Data Nasional). Pada *interview*

---

[1] 35 Kebocoran Data 2023, Kominfo Akui Cuma Beri Rekomendasi dan Teguran. (2023, Juni 19). Diakses pada Agustus 8, 2023 dari artikel : https://www.cnnindonesia.com/teknologi/20230619141948-192-963776/35-kebocoran-data-2023-kominfo-akui-cuma-beri-rekomendasi-dan-teguran.

[2] Sebanyak 34 juta data pemegang paspor Indonesia diduga 'bocor' – ‘Rakyat yang menderita, pemerintah paling dapat malu’. (2023, Juli 7) Diakses pada Agustus 8, 2023 dari artikel : https://www.bbc.com/indonesia/articles/c9e7e9grjmko

tersebut, *Chairman* Lembaga riset Keamanan Siber CISSReC Kominfo Pratama Persadha juga memvalidasi bahwa data-data yang beredar merupakan data paspor karena Ia merupakan salah satu korban dari sampel data yg bocor. Ia menambahkan bahwa adanya dugaan kasus ini akan membuat masyarakat mempertanyakan keamanan dari sistem yang dimiliki Imigrasi Indonesia.

Pada 10 Juli 2023, dalam *interview*-nya dengan CNBC Indonesia, Dirjen Imigrasi Kemenkumham Silmy Karim memberikan pernyataan bahwa *"Masyarakat tidak perlu terlalu khawatir terkait permasalahan kebocoran ini, karena tidak ditemukan adanya kebocoran data biometrik (sidik jari dan wajah) dan data yang bocor hanya berbentuk teks."* Beliau menjelaskan bahwa sejak tahun 2022, Imigrasi Indonesia sedang mendorong penggunaan paspor elektronik yaitu paspor dengan data biometrik. Paspor elektronik digunakan untuk meningkatkan keamanan (*level security)* data. Sehingga, apabila yang bocor adalah data teks, maka tidak akan berdampak apapun, karena di perlintasan yang digunakan adalah biometrik.

Pada 13 Juli 2023, melalui Siaran Pers Nomor: SP/IMI/007/2023/06, Dirjen Imigrasi Kemenkumham Silmy Karim memberikan pernyataan bahwa tim dari Direktorat Sistem dan Teknologi Informasi Keimigrasian (SISTIK) dan Direktorat Intelijen Keimigrasian Ditjen Imigrasi telah berkoordinasi dengan Kementerian Kominfo dan Badan Siber dan Sandi Negara (BSSN) dalam melakukan pemeriksaan pada elemen data terkait kebocoran *database.* Pada investigasi tersebut, ditemukan bahwa data yang mengalami kebocoran bukanlah data yang digunakan saat ini di Sistem Informasi Manajemen Keimigrasian (SIMKIM) Versi 2.0, melainkan data yang berlaku sebelum tahun 2021, maka dapat dipastikan bahwa tidak ada kebocoran data yang terjadi di tahun 2023. Secara teknis, kasus dugaan ini masih terus bergulir dan diselidiki sehingga dapat terjadi penambahan atau perubahan informasi pada masa mendatang. Melihat masifnya kasus kebocoran data pribadi yang terjadi dewasa ini, maka penting untuk dikaji aspek perlindungan hukum data pribadi menurut perspektif hukum Indonesia.

II. ISU

a) Bagaimana Urgensi Pelindungan Data Pribadi di Indonesia?
b) Bagaimana Perspektif Hukum Indonesia terhadap Pelindungan Data Pribadi?
c) Bagaimana Pelindungan, Pertanggungjawaban, dan Upaya Hukum Dalam Kasus Kebocoran Data 34 Juta Paspor WNI?

III. REGULASI

- Undang-Undang Dasar Negara Republik Indonesia 1945;
- Undang-Undang Nomor 39 Tahun 1999 Tentang Hak Asasi Manusia;
- Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi;
- Peraturan Pemerintah Nomor 82 Tahun 2012 Tentang Pelenyelenggaraan Sistem dan Transaksi Elektronik;
- Peraturan Pemerintah Nomor 71 Tahun 2019 Tentang Pelenyelenggaraan Sistem dan Transaksi Elektronik;

- Peraturan Pemerintah Nomor 80 Tahun 2019 Tentang Pedagangan Melalui Sistem Elektronik;
- *International Covenant on Civil and Political Rights* (ICCPR) Tahun 1966
- *ASEAN Declaration of Human Rights* Tahun 2012;
- *General Data Protection Regulation* (GDPR) Tahun 2016;

IV. ANALISIS

a. Urgensi Pelindungan Data Pribadi di Indonesia

Data Pribadi adalah setiap data tentang seseorang yang teridentifikasi dan/atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui Sistem Elektronik dan/atau nonelektronik.[3] Insiden kebocoran data merupakan insiden siber, dimana data atau rahasia milik organisasi telah diakses dan diungkap ke publik oleh *threat actor* tanpa sepengetahuan dari pemilik sistem. Data-data yang diambil oleh penyerang umumnya bersifat sensitif, seperti *Personal Identifiable Information* (PII), data sensitif organisasi, dan data lainnya yang seharusnya hanya diketahui oleh pihak yang memiliki hak.

Dewasa ini, informasi perihal dugaan kebocoran data kerap kali terdengar di telinga. Berdasarkan hasil kajian perusahaan keamanan siber Surfshark, Indonesia menjadi negara ketiga dengan jumlah kebocoran data terbanyak di dunia. Sebanyak 12,74 juta data akun mengalami kebocoran selama kuartal III tahun 2022.[4] Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) juga mengungkapkan bahwa peningkatan terhadap penetrasi pengguna internet di Indonesia dalam rentang waktu tahun 2019 hingga 2020 diikuti dengan peningkatan berbagai kasus data pribadi. Tingkat penetrasi pengguna internet mencapai 190 juta dari keseluruhan jumlah penduduk yakni 266 juta orang, yang mana telah menyentuh 73,7% warga Indonesia. Berdasarkan laporan terbaru dari *National Cyber Security Index* (NCSI), tingkat keamanan siber Indonesia berada di peringkat 84 dengan poin 38,96. Data tersebut menunjukan betapa peliknya kondisi keamanan siber di Indonesia yang kerap dilanda kebocoran data.

Pernyataan *"Masyarakat tidak perlu terlalu khawatir karena kebocoran terjadi pada data lama dan hanya data yang berbentuk teks"* yang dilontarkan Dirjen Imigrasi Kemenkumham Silmy Karim menyebabkan timbulnya pertanyaan baru yaitu 'Apakah masyarakat benar-benar tidak perlu khawatir terkait hal ini?' Hal tersebut telah terjawab beberapa tahun sebelumnya pada salah satu *interview* antara Kompas TV dengan Ketua Lembaga Riset Keamanan Siber CISSReC Pratama Persadha pada 25 Mei 2021 yang sedang membahas mengenai kasus dugaan kebocoran 279 juta data pengguna Badan Penyelenggara Jaminan Sosial (BPJS) Kesehatan. Pratama Persadha mengatakan bahwa banyak sekali potensi kejahatan yang dapat dilakukan oleh pelaku pembocoran data yang

---

[3] Pasal 1 Angka 29 Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

[4] Vika Azkiya Dihni, "Kasus Kebocoran Data di Indonesia Melonjak 143% pada Kuartal II 2022," Databoks, 2022, diakses pada https://databoks.katadata.co.id/datapublish/2022/08/09/kasus-kebocorandata-di-indonesia-melonjak-143-pada-kuartal-ii-2022.

memiliki nama lengkap, nomor *handphone,* tanggal lahir, dan alamat dari korban kebocoran data. Adapun potensi-potensi kejahatan yang dapat dilakukan, yaitu:

1. Spam iklan yang tidak diinginkan, seperti spam telepon dari pinjaman *online* dan tawaran-tawaran asuransi;
2. Penipuan, kepemilikan data-data pribadi korban mempermudah penipu untuk melancarkan aksinya;
3. Kebocoran data nomor telepon mempermudah menautkannya ke *E-wallet*. Setelah menautkan *link*, pelaku kejahatan dapat pula mengetahui Nomor Induk Kependudukan (NIK) korban. Hal tersebut, akan mempermudah pelaku kejahatan melakukan *take over* akun dengan menggunakan *social engineering,* bahkan dapat dengan mudah melakukan *take over* rekening bank;
4. Perdagangan data pribadi di *market place*.

Dalam kesempatan yang sama, Anggota Komisi IX DPR Netty Prasetiyani juga menyatakan bahwa kasus kebocoran data seperti ini sudah masuk ke dalam ranah ancaman kedaulatan negara karena ketika data pribadi sudah tidak aman, peluang untuk memalsukan dan menyalahgunakan data tersebut untuk berbagai kepentingan semakin terbuka lebar.[5] Maka, dapat disimpulkan bahwa kasus kebocoran data merupakan permasalahan yang sangat krusial dan merugikan berbagai pihak, terkhususnya bagi korban. Pemerintah perlu melihat adanya urgensi pelindungan data pribadi masyarakat dan memberikan perhatian lebih pada keamanan siber Indonesia guna:

1. Melindungi keamanan rakyat Indonesia;
2. Meminimalisir ancaman;
3. Meminimalisir gangguan pada ketersediaan (*availability*);
4. Menjaga integritas (*integrity*) dan kerahasiaan (*confidentiality*) sebuah informasi; serta
5. Mencegah terjadinya serangan pada jaringan komputer (perangkat keras dan perangkat lunak) terkait informasi di dalamnya dan elemen-elemen ruang siber lainnya.

b. Perkembangan dan Perspektif Hukum Indonesia terhadap Pelindungan Data Pribadi

Privasi dan data pribadi bukanlah istilah yang baru. Pada awalnya, pelindungan ‘data pribadi’ tidak dengan tegas disebutkan dalam *International Covenant on Civil and Political Rights* (ICCPR) tahun 1966. Indonesia telah meratifikasi ICCPR pada 28 Oktober 2005 melalui Undang-Undang Nomor 12 Tahun 2005 Tentang Pengesahan *International Covenant On Civil and Political Rights* (Kovenan Internasional Tentang Hak-Hak Sipil dan Politik). Regulasi tersebut secara substansial menjelaskan pelindungan terhadap data pribadi merupakan bagian dari privasi atau kehidupan pribadi setiap orang. Seiring dengan waktu, istilah pelindungan ‘data pribadi’ diatur secara jelas, baik dalam

[5] Netty Prasetiyani, “Ahli Keamanan Siber Ungkap Dampak dan Bahaya dari Kebocoran Data Penduduk Indonesia”, Video Youtube, 25 Mei 2021, KOMPASTV, 9.41 hingga 14.55, https://youtu.be/gyShF5Cd_Fk?si=2OhF3qZIDOsr3f0L

konvensi regional maupun peraturan perundang-undangan. Salah satu konvensi regional tingkat ASEAN yang mengatur mengenai data pribadi sebagai bagian dari hak asasi manusia adalah *ASEAN Declaration of Human Rights* (2012). Pasal 21 deklarasi tersebut menyatakan: *"Every person has the right to be free from arbitrary interference with his or her privacy, family, home or correspondence including* ***personal data****, or to attacks upon that person's honour and reputation. Every person has the right to the protection of the law against such interference or attacks.*"

Indonesia mengatur pelindungan data pribadi sebagai hak konstitusional yang diatur dalam Pasal 28G ayat (1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 (UUD NRI 1945), yang menjelaskan bahwa "*Setiap orang berhak atas* ***perlindungan diri pribadi****, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya, serta berhak atas rasa aman dan pelindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi*." Sehingga, apabila dikaitkan, regulasi ini menegaskan bahwa setiap warga negara tanpa terkecuali berhak atas pelindungan data pribadi meliputi seluruh pemrosesan data pribadi yang mulai dari pengumpulan, penggunaan, penyimpanan, pengiriman, hingga penghapusan.

Pelindungan data pribadi dalam perjalanannya diatur dalam beberapa peraturan perundang-undangan. Terutamanya Peraturan Pemerintah (PP) No. 71 Tahun 2019 dan PP No. 80 Tahun 2019 yang juga mengatur aspek pelindungan data pribadi, maka setiap penyelenggara sistem elektronik selayaknya memenuhi kepatuhan hukum atas pelindungan data pribadi yang ditentukan dalam peraturan perundang-undangan tersebut. Dalam kedua PP tersebut diuraikan asas-asas pelindungan data pribadi berdasarkan kelaziman *(best practices)* yang telah diakomodir dalam Pasal 2 ayat (5) PP No. 71/2019 dan Pasal 33 PP No. 80/2019, serta juga terdapat ancaman sanksi administratif terhadap ketidakpatuhan atas aturan tersebut.[6] Barulah pada tahun 2022 ketentuan mengenai Pelindungan Data Pribadi diatur khusus dalam UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP).

[6] Makarim, E. (2020). *Pertanggungjawaban Hukum Terhadap Kebocoran Data Pribadi.* https://www.hukumonline.com/berita/a/pertanggungjawaban-hukum-terhadap-kebocoran-data-pribadi-lt5f067836b37ef/?page=1

Pengesahan Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi (UU PDP) membawa angin segar di tengah kekhawatiran publik akibat maraknya kasus kebocoran data di internet. Undang-Undang ini berfungsi menjadi landasan dalam menjaga serta menjamin kehormatan dan kedaulatan data pribadi. Pasal 1 angka 1 Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi (UU PDP), yaitu "*Data Pribadi adalah data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik atau nonelektronik."* Penjelasan terkait jenis data pribadi diatur dalam *General Data Protection Regulation* (GDPR) bahwa "*The following personal data is considered 'sensitive' and is subject to specific processing conditions: a) personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs; b) trade-union membership; c) genetic data, biometric data processed solely to identify a human being; d) health-related data; e) data concerning a person's sex life or sexual orientation*" Maka dari itu, dapat dikatakan bahwa data pribadi merupakan informasi perihal subjek data yang menyangkut informasi umum seperti nama, umur, jenis kelamin, alamat, serta informasi privat lainya yang harus dilindungi.

Undang-undang tersebut mengatur hal-hal penting seperti kategorisasi data, seperti tercantum dalam Pasal 4 UU PDP, berbunyi "*Data Pribadi terdiri atas: a. Data Pribadi yang bersifat spesifik; dan b. Data pribadi yang bersifat umum*". Kemudian, jenis data pribadi dan hak subjek data pribadi yang tertuang dalam Pasal 5 hingga Pasal 15 UU PDP. Kewajiban pengendali data pribadi dan prosesor dalam pemrosesan data pribadi yang dijelaskan dalam Pasal 20 hingga Pasal 50 UU PDP. Undang-undang ini juga menegaskan bahwa pembentukan lembaga pelindungan data pribadi akan bertanggung jawab langsung kepada Presiden yang termuat dalam Pasal 58 hingga Pasal 60 UU PDP.

Selain itu, Siti Yuniarti dalam diskusi implementasi UU PDP di masing-masing sektor yang diselenggarakan oleh Kementerian Komunikasi dan Informatika (KOMINFO), menjelaskan terdapat 10 ketentuan yang mengatur aturan turunan dalam pelaksanaan pembentukan aturan turunan dalam UU PDP yang berpotensi untuk dimasukan dalam peraturan pelaksana UU PDP, antara lain: (1) pengajuan keberatan atas pemrosesan secara otomatis; (2) pelanggaran pemrosesan data pribadi dan tata cara pengenaan ganti rugi; (3) hak subjek data pribadi untuk menggunakan dan mengirimkan data pribadi; (4) pelaksanan pemrosesan data pribadi; (5) penilaian dampak pelindungan data pribadi; (6) tata cara pemberitahuan; (7) pejabat atau petugas yang melaksanakan fungsi pelindungan data pribadi; (8) transfer data pribadi; (9) tata cara pengenaan sanksi administratif; dan (10) tata cara pelaksanaan wewenang lembaga dan aturan pelaksanaan UU PDP. [7]

Hak Privasi merupakan hak konstitusional yang melekat dalam setiap warga negara, adanya hak tersebut mengharuskan negara menjalankan peranya sebagai *the duty*

[7] Yuniarti, S. (2023). Diskusi Implementasi UU PDP di Masing-Masing Sektor. Kementerian Komunikasi dan Informatika (KOMINFO). Tanggal 16 Februari 2023

bearer dalam melindungi hak setiap warganya. Pasal 1 Angka (2) UU PDP menegaskan bahwa "*Pelindungan data pribadi merupakan keseluruhan upaya untuk melindungi data pribadi dalam rangkaian pemrosesan data pribadi guna menjamin hak konstitusional subjek data pribadi*". Regulasi yang tertuang dalam UU PDP menjelaskan kewajiban dalam pengendalian suatu data yang dimaksudkan dalam hal ini adalah data pribadi menjadi luas. Oleh sebab itu, terdapat beberapa prinsip yang termuat dalam UU PDP, yaitu:[8]

1. Pengumpulan secara terbatas, spesifik, sah dan transparan (Pasal 27 UU PDP);
2. Dilakukan sesuai dengan tujuan yang termuat dalam UU PDP (Pasal 28 UU PDP);
3. Menjamin hak subjek data (Pasal 11, Pasal 12 dan Pasal 13 UU PDP);
4. Akurat, lengkap, tidak menyesatkan, mutakhir, dan dapat di pertanggungjawabkan;
5. Melindungi dan memastikan keamanan data pribadi, dalam melakukan pemrosesan suatu data pengendali wajib memastikan keamanan dari data yang akan di proses. Hal ini dilakukan agar pemrosesan data yang dilakukan oleh pengendali data dilakukan dengan ketentuan UU PDP (Pasal 35 UU PDP);
6. Memberikan pemberitahuan tujuan, aktivitas pemrosesan dan kegagalan pelindungan;
7. Melakukan penghapusan dan pemusnahan berdasar masa retensi atau permintaan, serta;
8. Bertanggungjawab dan dibuktikan secara jelas.

Regulasid dalam UU PDP telah mengatur larangan serta sanksi dalam penyalahgunaan data pribadi. Adapun larangan dalam UU PDP, yaitu:

1. Larangan untuk memperoleh atau mengumpulkan data pribadi yang bukan milikinya dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian subjek data pribadi;
2. Larangan untuk mengungkapkan data pribadi yang bukan miliknya;
3. Larangan untuk menggunakan data pribadi yang bukan miliknya;
4. Larangan untuk membuat data pribadi palsu atau memalsukan data pribadi dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian bagi orang lain.

UU PDP juga memuat sanksi-sanksi atas pelanggaran pelindungan data pribadi yang terdiri dari sanksi administratif pada pasal 51 UU PDP dan sanksi pidana pada pasal 67 hingga pasal 68 UU PDP. Selain itu, sanksi pidana dapat dikenakan korporasi hanya berupa denda dengan ketentuan paling banyak 10 kali dari maksimal pidana denda yang diancamkan. Adapun pidana lain yang dikenakan korporasi selain pidana denda termuat dalam Pasal 70 ayat (4) UU PDP.

[8] Sianipar, M. L. (2023). *Implementasi Kewajiban To Protect Atas Data Pribadi Sebagai Hak Asasi Manusia Dalam Perspektif UU No 27 Tahun 2022 Tentang Pelindungan Data Pribadi* (Doctoral dissertation).

Maka dari itu, segala kewajiban dari pengendali data harus dimaknai sebagai wujud dari tindakan negara dalam melindungi hak atas data pribadi setiap orang, dikarenakan data pribadi merupakan hak privat yang harus dilindungi oleh negara sebagaimana amanat Pasal 28G ayat (1) UUD NRI 1945. Sebagaimana diketahui data pribadi dikendalikan atau dikelola oleh pengendali data, sehingga dapat memberikan rekognisi pemilik data serta memberikan pelindungan bagi setiap orang sebagai salah satu pemenuhan hak asasi manusia. Lahirnya UU PDP bukanlah sebagai finalisasi dari perjuangan pelindungan data di Indonesia. Pembenahan, penegakan dan sinkronisasi regulasi masih perlu dilakukan demi menciptakan ekosistem data pribadi yang aman di Indonesia.

c. Pelindungan, Pertanggungjawaban, dan Upaya Hukum Dalam Kasus Kebocoran Data 34 Juta Paspor WNI

1. Perlindungan Hukum

Kasus kebocoran data berupa nomor paspor, NIKIM (National Identiti Kartu Identitas Masyarakat yang memuat nama, alamat, nomor KTP, dan NPWP), tanggal pembuatan dan tanggal kadaluarsa paspor, tanggal lahir, jenis kelamin, dan pemutakhiran. Berdasarkan kualifikasi jenis data pribadi pada Pasal 2 UU PDP, data-data tersebut tergolong pada data pribadi yang bersifat umum. Hal ini berarti data yang mengalami kebocoran masih di dalam ranah data pribadi yang dilindungi oleh UU PDP. Terduga pelaku pembocoran data adalah seorang pemilik akun anonim bernama “Bjorka”. Terjadinya kebocoran data tersebut mengindikasikan telah terbobolnya sistem ketika proses migrasi data dari penyimpanan di Imigrasi ke PDN. Terbobolnya sistem sehingga terjadi kebocoran data mengindikasikan ketidakmampuan Pengendali Data Pribadi dalam menjaga keamanan data pribadi dari pengaksesan yang tidak sah.

Dalam UU PDP dijelaskan bahwa Pengendali Data Pribadi adalah setiap orang, badan publik, dan organisasi internasional yang bertindak sendiri-sendiri atau bersama-sama dalam menentukan tujuan dan melakukan kendali pemrosesan data pribadi. Pemrosesan data pribadi dalam Pasal 16 UU PDP meliputi hal-hal seperti penampilan, pengumuman, transfer, penyebarluasan, atau pengungkapan data pribadi. Makna ‘transfer’ data pribadi dapat disamakan dengan istilah ‘migrasi’ dalam kasus tersebut.

Pemrosesan data pribadi dalam Pasal 16 UU PDP dilakukan sesuai dengan prinsip Pelindungan Data Pribadi, yang salah satunya adalah asas pemrosesan data pribadi yang dilakukan dengan melindungi keamanan data pribadi dari pengaksesan dan pengungkapan yang tidak sah. Pasal 38 UU PDP juga menegaskan kewajiban Pengendali Data Pribadi untuk melindungi data pribadi dari pemrosesan yang tidak sah. Lebih lanjut, Pasal 39 UU PDP menjelasakan bahwa Pengendali Data Pribadi wajib mencegah data pribadi diakses secara tidak sah. Dalam hal ini Pengendali data pribadi wajib melakukan pencegahan dengan menggunakan sistem keamanan terhadap Data Pribadi yang diproses dan/ atau memproses Data Pribadi sistem elektronik secara andal, aman, dan bertanggung jawab.

Pasal 55 UU PDP mewajibkan pengendali data pribadi yang melakukan dan menerima transfer data pribadi melakukan pelindungan. Berdasarkan uraian di atas, masyarakat sebagai subjek data pribadi berhak menerima pelindungan termasuk dalam proses pentransferan data pribadi. Pengendali Data Pribadi yang dalam hal ini adalah badan publik yaitu Ditjen Imigrasi dan Kominfo sebagai penyelenggara dari Pusat Data Nasional (PDN) yang terlibat dalam proses transfer data pribadi wajib melindungi data pribadi tersebut. Namun, tampaknya kewajiban untuk melindungi data pribadi belum terlaksana dengan baik sehingga terjadi kebocoran. Oleh karena itu, terdapat pertanggungjawaban atas dugaan kasus kebocoran data paspor 34 juta Warga Negara Indonesia (WNI)

2. Pertanggungjawaban Hukum

Pertanggungjawaban hukum dalam UU PDP dapat berupa sanksi administratif ataupun sanksi pidana. Sanksi administratif dalam UU PDP ditujukan kepada Pengendali Data Pribadi dan Prosesor Data Pribadi yang gagal dalam melaksanakan kewajibannya, kewajiban yang dimaksud seperti melindungi data pribadi dari akses yang tidak sah, melindungi data pribadi ketika terjadi proses transfer data pribadi, dan kewajiban-kewajiban lain yang sebagaimana diatur dalam Pasal 57 ayat (1) UU PDP. sedangkan sanksi pidana ditujukan kepada setiap orang pelaku tindak kejahatan pelindungan data pribadi. Pasal 51 UU PDP mengatur mengenai sanksi administratif, yaitu berupa:

a. peringatan tertulis;
b. penghentian sementara kegiatan pemrosesan Data Pribadi;
c. penghapusan atau pemusnahan Data Pribadi; dan/atau
d. denda administratif.

Sanksi administratif tersebut dijatuhkan oleh lembaga pelindungan data pribadi. Sementara itu, ketentuan pidana pelindungan data pribadi diatur dalam Pasal 67 dan 68 UU PDP atas tindak pidana kejahatan data pribadi yang berupa pengumpulan data pribadi secara melawan hukum, pengungkapan data pribadi secara melawan hukum, penggunaan data pribadi yang bukan miliknya, serta pembuatan atau pemalsuan data pribadi.

Dalam kasus tersebut, seharusnya dilakukan penjatuhan sanksi administratif kepada Pengendali Data Pribadi yang bersangkutan karena telah gagal dalam menjalankan kewajibannya untuk menjaga data pribadi ketika dilakukan proses transfer data sehingga terjadi kebocoran data pribadi. Sementara Terduga pelaku pada kasus tersebut yaitu pemilik akun anonim bernama “Bjorka” seharusnya dikenakan pidana karena telah mengungkapkan data pribadi berupa 1.000.000 sampel data nama pengguna paspor serta mencoba memperjualbelikan 34.900.867 data nama pengguna paspor yang seharga $10.000 USD atau sekitar Rp150.000.000,00 *(seratus lima puluh juta rupiah)*. Tindakan terduga pelaku tersebut telah melanggar ketentuan yang terdapat pada:

1. Pasal 67 ayat (1) UU PDP yang menyatakan: *“Setiap Orang yang dengan sengaja dan melawan hukum memperoleh atau mengumpulkan Data Pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain yang*

dapat mengakibatkan kerugian Subjek Data Pribadi sebagaimana dimaksud dalam Pasal 65 ayat (1) dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau pidana denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah)"

2. Pasal 67 ayat (2) UU PDP yang menyatakan: "*Setiap Orang yang dengan sengaja dan melawan hukum mengungkapkan Data Pribadi yang bukan miliknya sebagaimana dimaksud dalam Pasal 65 ayat (2) dipidana dengan pidana penjara paling lama 4 (empat) tahun dan/atau pidana denda paling banyak Rp4.000.000.000,00 (empat miliar rupiah)".*

3. Upaya Hukum

UU PDP mengatur upaya-upaya hukum yang dapat dilakukan oleh subjek data pribadi atas peristiwa pelanggaran data pribadi maupun jika terjadi sengketa data pribadi. Dalam Pasal 12 UU PDP diatur bahwa subjek data pribadi berhak menggugat dan menerima ganti rugi atas pelanggaran pemrosesan data pribadi tentang dirinya sesuai dengan ketentuan peraturan perundang-undangan. Dimana ketentuan mengenai pelanggaran pemrosesan data pribadi dan tata cara pengenaan ganti rugi diatur dalam Peraturan Pemerintah. Adapun dasar gugatan ganti rugi ini adalah sebagaimana yang terdapat dalam Pasal 1365 Kitab Undang-Undang Hukum Perdata.

UU PDP juga mengatur ketentuan mengenai penyelesaian sengketa pelindungan data pribadi. Pasal 64 UU PDP menyatakan bahwa penyelesaian sengketa pelindungan data pribadi dilakukan melalui arbitrase, pengadilan, atau lembaga penyelesaian sengketa alternatif lainnya sesuai dengan ketentuan peraturan perundang-undangan. Hukum acara yang berlaku di dalamnya adalah hukum acara sesuai dengan ketentuan peraturan perundang-undangan. Perbedaannya adalah dalam sengketa pelindungan data pribadi terdapat alat bukti tambahan selain alat bukti yang disebutkan dalam hukum acara, yaitu alat bukti lain berupa informasi elektronik dan/ atau dokumen elektronik sesuai dengan ketentuan peraturan perundang-undangan. Perbedaan lainnya adalah dalam proses persidangan dapat dilakukan secara tertutup jika diperlukan untuk melindungi data pribadi.

Mengingat besarnya kasus kebocoran data pribadi tersebut, yang mana mencapai jutaan data pribadi masyarakat, maka upaya hukum yang dapat dilakukan adalah dengan mengajukan gugatan *class action.* Dimana dalam gugatan *class action* seluruh korban akan diwakili oleh perwakilannya dalam persidangan. Gugatan melawan hukum dapat diajukan kepada pemerintah yaitu terhadap Ditjen Imigrasi dan Kominfo sebagai penyelenggara dari Pusat Data Nasional (PDN) sebagai pihak Pengendali Data Pribadi yang terlibat dalam proses transfer data pribadi yang mengalami kebocoran. Pelaporan kasus kebocoran data pribadi.

V. KESIMPULAN

1. Banyaknya insiden kebocoran data yang terjadi menunjukan urgensi pelindungan data pribadi di Indonesia. Pada kuartal III tahun 2022 terdapat 12,74 juta data akun mengalami

kebocoran. Maka dari itu, perlindungan data pribadi menjadi hal yang *urgent* untuk dijaga oleh pemerintah guna melindungi keamanan rakyat, meminimalisir ancaman, meminimalisir gangguan pada ketersediaan (*availability*), menjaga integritas (*integrity*) dan kerahasiaan (*confidentiality*) sebuah informasi, dan mencegah terjadinya serangan pada jaringan komputer (perangkat keras dan perangkat lunak) terkait informasi di dalamnya dan elemen-elemen ruang siber lainnya.

2. Pengesahan Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi (UU PDP) menjadi dasar perlindungan hak privat yang merupakan hak konstitusional. Undang-undang ini menjelaskan 10 ketentuan yang mengatur aturan turunan dalam pelaksanaan pembentukan aturan turunan dalam UU PDP yang berpotensi untuk dimasukan dalam peraturan pelaksana UU PDP, antara lain: (1) pengajuan keberatan atas pemrosesan secara otomatis; (2) pelanggaran pemrosesan data pribadi dan tata cara pengenaan ganti rugi; (3) hak subjek data pribadi untuk menggunakan dan mengirimkan data pribadi; (4) pelaksanan pemrosesan data pribadi; (5) penilaian dampak pelindungan data pribadi; (6) tata cara pemberitahuan; (7) pejabat atau petugas yang melaksanakan fungsi pelindungan data pribadi; (8) transfer data pribadi; (9) tata cara pengenaan sanksi administratif; dan (10) tata cara pelaksanaan wewenang lembaga dan aturan pelaksanaan UU PDP. Pengimplementasian UU PDP.
3. Berdasarkan Pasal 2 UU PDP, data-data yang bocor dalam dugaan kasus tersebut tergolong pada data pribadi yang bersifat umum dan keberadaannya dilindungi oleh UU PDP. Pasal 39 UU PDP menjelasakan bahwa yang wajib mencegah pengaksesan data pribadi secara tidak sah adalah Pengendali Data Pribadi, yang dalam kasus tersebut adalah Ditjen Imigrasi dan Kominfo sebagai penyelenggara dari Pusat Data Nasional (PDN). Namun, tampaknya kewajiban untuk melindungi data pribadi belum terlaksana dengan baik sehingga terjadi kebocoran. Oleh karena itu, terdapat pertanggungjawaban yang harus diberikan oleh Pengendali data pribadi atas kebocoran data dan upaya hukum yang dapat dilakukan oleh korban dari kebocoran data seperti sanksi administratif dan sanksi pidana yang ketentuannya telah termuat di dalam UU PDP.

DAFTAR PUSTAKA

Peraturan Perundang-undangan

Undang-Undang Dasar Negara Republik Indonesia 1945.

Undang-Undang Nomor 39 Tahun 1999 Tentang Hak Asasi Manusia.

Undang-Undang Nomor 12 Tahun 2005 Tentang Pengesahan *International Covenant On Civil and Political Rights* (Kovenan Internasional Tentang Hak-Hak Sipil dan Politik).

Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi.

Peraturan Pemerintah Nomor 82 Tahun 2012 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik;

Peraturan Pemerintah Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik;

Peraturan Pemerintah Nomor 80 Tahun 2019 Tentang Perdagangan Melalui Sistem Elektronik;

Konvensi

International Covenant on Civil and Political Rights

ASEAN Declaration of Human Rights

General Data Protection Regulation

Buku

Badan Siber dan Sandi Negara. 2023. Lanskap Keamanan Siber Indonesia 2022.

Artikel/Jurnal

Chandraditya, E. (2022). Tanggung Jawab Pemerintah Atas Kebocoran Data pada Aplikasi Peduli Lindungi.

Internet

BBC News Indonesia. (Juli 2023, 7). *Sebanyak 34 juta data pemegang paspor Indonesia diduga 'bocor' – 'Rakyat yang menderita, pemerintah paling dapat malu'.* https://www.bbc.com/indonesia/articles/c9e7e9grjmko

CNBC Indonesia. (Juli 2023, 10). *34 Juta Data Paspor Bocor, Dirjen Imigrasi: Masih Dugaan!*https://www.cnbcindonesia.com/news/20230708130632-8-452460/34-juta-data-paspor-bocor-dirjen-imigrasi-masih-dugaan

Widi, Shilvina. (Juli 2023, 6). *Deret Kasus Kebocoran Data RI pada 2023, dari BSI hingga Paspor.* https://dataindonesia.id/digital/detail/deret-kasus-kebocoran-data-ri-pada-2023-dari-bsi-hingga-paspor

Vika Azkiya Dihni, "Kasus Kebocoran Data di Indonesia Melonjak 143% pada Kuartal II 2022," Databoks, 2022, diakses pada https://databoks.katadata.co.id/datapublish/2022/08/09/kasus-kebocorandata-di-indonesia-melonjak-143-pada-kuartal-ii-2022.

Silmy, Karim. 2023. Press Release. Batam : Kantor Imigrasi Kelas I khusus TPI Batam.

Semuel, A. Pangerapan. Press Release. Kementerian Komunikasi dan Informatika.