BAB I
PENDAHULUAN

1.1 Latar Belakang

Zaman yang semakin maju seperti saat ini membuat segala sesuatu bisa diakses hanya dengan internet, dengan kebebasan yang ada sekarang dan didukung oleh perangkat elektronik yang praktis seperti komputer, smartphone sampai dengan jaringan yang bagus, memudahkan orang untuk bisa mengakses segala hal termasuk data pribadi orang lain (Kautsar, 2023). Menurut Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), jumlah orang yang terhubung dengan internet di Indonesia sudah mencapai 78,19 persen pada tahun 2023 atau sekitar 215.626.156 orang dari total penduduk yang berjumlah 275.773.901 orang. Pada tahun ini, penetrasi internet di Indonesia naik sebesar 1,17 persen (APJII, 2023). Kenaikan penetrasi ini masih dipengaruhi oleh penggunaan internet yang semakin jadi keperluan masyarakat, terutama sejak pandemi Covid-19 pada tahun 2020.

Dengan meningkatnya pengguna internet di Indonesia itu juga berdampak pada privasi data pribadi dari pengguna internet di Indonesia. Seperti kasus yang terjadi pada aplikasi Tokopedia dimana mengalami kebocoran data, kebocoran data adalah suatu kondisi dimana data sensitif secara sengaja atau tidak sengaja terexpose atau terakses oleh pihak tidak sah. Pada bulan maret 2020 tokopedia mengalami kebocoran data yang menyebabkan 91 juta akun pengguna Tokopedia dan 7 juta akun pedagang mengalai kebocoran yang diakibaktan serangan peratas yang selanjutnya dijual di *website darkweb*, data yang bocor dan dijual adalah data

nama, *user id*, *password*, nomer hp, jenis kelamin, dan juga tanggal lahir (CNN Indonesia, 2020).

Tidak hanya kasus tersebut, pada tahun 2020 sampai dengan 2023 sering terjadi kebocoran data akibat serangan dari peretas, salah satu peretas yang terkenal bernama Bjorka, pada tahun 2022 Bjorka telah meretas *history browsing* pelanggan Indihome, data yang bocor sebanyak 26 juta data dimulai dari nama, jenis kelamin, *keyword*, serta Nomor Induk Kependudukan (NIK) para pelanggan Indihome. Selanjutnya kebocoran data Kementerian Komunikasi dan Informatika (Kominfo) yaitu registrasi SIM Card sebanyak 1,3 miliar data. Pada tanggal 6 september 2022, 105 juta data pemilih bocor yang berasal dari Komisi Pemilihan Umum (KPU), bahkan dokumen rahasia milik Presiden Jokowi juga bocor, dokumen tersebut didapat dari Badan Intelijen Negara (BIN).

Selanjutnya Bjorka menyebarkan data para pejabat di Indonesia diantaranya:

1. Menteri Komunikasi dan Informatika (Menkominfo), Johnny G Plate
2. Ketua Dewan Perwakilan Rakyat (DPR), Puan Maharani
3. Direktur Jenderal Aplikasi Informatika Kominfo, Semuel Abrijani Pangerapan
4. Menteri Koordinator Bidang Kemaritiman dan Investasi Indonesia, Luhut Binsar Pandjaitan
5. Menteri Badan Usaha Milik Negara, Erick Thohir

Data yang dibocorkan adalah nama, alamat rumah, nama orang tua, nomor kartu keluarga (KK), nomor kartu tanda penduduk (KTP), agama, riwayat

pendidikan, nomer telepon, dan masih banyak lagi (Dewi, 2022). Lalu ada kasus dari Dr Tirta. Dr Tirta adalah seorang pengusaha dan influencer di media sosial yang dikenal sebagai salah satu tokoh yang peduli dengan kesehatan masyarakat. Namun, pada tanggal 31 januari 2022 dia mendapat kabar dari orang tuanya di Solo. Ternyata, ada oknum yang datang ke rumahnya dan menagih utang sebesar Rp 288.000 dengan mengaku sebagai petugas pinjol (pinjaman online). Dr Tirta merasa bingung karena dia tidak pernah meminjam uang dari pinjol apapun. Setelah ditelusuri sumber masalahnya, dia menemukan bahwa data pribadinya, termasuk KTP bocor dan disalahgunakan oleh orang lain untuk mengajukan pinjaman online. Akhinya hal ini dilaporkan ke pihak pinjol dan Kominfo. (Sumarni, 2022)

Dikutip laman website Kementerian Komunikasi dan Informatika Republik Indonesia, Dirjen Aplikasi dan Informatika (Aptika) Semuel Abrijani mengatakan setidaknya ada 5 hal yang menjadikan mengapa data pribadi perlu dilindungi yakni:

1. Intimidasi online terkait gender, data pribadi berupa jenis kelamin patut dilindungi untuk menghindari kasus pelecehan seksual atau perundungan (bullying) secara online. Perlindungan terhadap data penting dilakukan agar menghindari ancaman kejahatan dunia maya termasuk Kekerasan Berbasis Gender Online (KBGO).
2. Mencegah penyalahgunaan data pribadi oleh pihak yang tidak bertanggung jawab.
3. Menjauhi potensi penipuan.
4. Menghindari potensi pencemaran nama baik.
5. Hak kendali atas data pribadi, secara global kita memiliki kontrol atas privasi data pribadi kita. Hal itu sudah dijamin dalam Deklarasi Universal

tentang Hak Asasi Manusia 1948 pasal 12 dan Konvensi Internasional tentang Hak Sipil dan Politik (ICCPR) 1966 pasal 17, Indonesia pun sudah meratifikasi keduanya. Data pribadi termasuk hak asasi dan privasi yang tercantum dalam Deklarasi Universal Manusia 1948 Pasal 12. Data pribadi merupakan aset atau komoditas bernilai tinggi di era *big data* dan ekonomi digital (KOMINFO, 2019).

Ada beberapa faktor yang menyebabkan data pribadi bocor di Indonesia, namun ada 3 faktor yang paling utama, yaitu: pertama, faktor Standar Operasional Prosedur (SOP), kedua, faktor Sumber Daya Manusia (SDM) dan ketiga, faktor Teknologi (Lahur, 2022).

Faktor Standar Operasional Prosedur (SOP):

1. Ketidaksesuaian SOP: Banyak organisasi atau lembaga di Indonesia mungkin memiliki SOP yang tidak memadai atau tidak diterapkan dengan benar. Misalnya, dalam perusahaan yang tidak memiliki SOP yang ketat dalam mengelola dan melindungi data pribadi, risiko kebocoran data menjadi lebih besar.
2. Ketidaktransparan dan lemahnya regulasi: Kurangnya regulasi yang ketat dan transparan dalam mengatur perlindungan data pribadi dapat menyebabkan SOP yang lemah. Organisasi mungkin tidak merasa terdorong untuk mengimplementasikan langkah-langkah yang memadai untuk melindungi data pribadi.

Faktor Sumber Daya Manusia (SDM):

1. Pelatihan yang kurang: Kurangnya pelatihan bagi petugas mengenai pentingnya keamanan data dan tindakan yang harus diambil dalam melindungi data pribadi dapat menyebabkan kesalahan manusia yang mengarah pada kebocoran data.
2. Penyusupan atau kolusi: Beberapa kasus kebocoran data yang disebabkan oleh petugas yang dengan sengaja atau tidak sengaja membagikan data pribadi dengan pihak ketiga atau melibatkan diri dalam tindakan yang merugikan perusahaan.

Faktor Teknologi:

1. Keamanan TI yang lemah: Jika sistem dan perangkat lunak yang digunakan oleh sebuah organisasi memiliki keamanan yang lemah, maka data pribadi dapat lebih mudah diakses oleh pihak yang tidak berwenang. Contoh-contoh termasuk kekurangan pembaruan perangkat lunak, konfigurasi yang buruk, dan ketidakmampuan untuk mendeteksi serangan siber.
2. Serangan siber: Penyusupan oleh peretas atau serangan siber dapat menjadi penyebab kebocoran data. Penyerang dapat mencuri data pribadi atau merusak sistem, yang dapat mengakibatkan kebocoran data.

Perlindungan data pribadi dalam sistem elektronik meliputi perlindungan terhadap segala aktivitas yang berkaitan dengan data pribadi, seperti: pengambilan, pengumpulan, pengolahan, penganalisisan, penyimpanan, penampilan,

pengumuman, pengiriman, penyebarluasan, dan pemusnahan data pribadi. Hal ini diatur dalam Peraturan Menteri Komunikasi Dan Informatika Nomor 20 Tahun 2016 Tentang Perlindungan Data Pribadi Dalam Sistem Elektronik.

Didalam pasal yang sama, juga dibahas bahwa pelaksanaan ketentuan perlindungan data pribadi itu meliputi :

1. Penghormatan terhadap Data Pribadi sebagai privasi.
2. Data Pribadi bersifat rahasia sesuai Persetujuan dan/atau berdasarkan ketentuan peraturan perundang-undangan.
3. Berdasarkan Persetujuan.
4. Relevansi dengan tujuan perolehan, pengumpulan, pengolahan, penganalisisan, penyimpanan, penampilan, pengumuman, pengiriman, dan penyebarluasan.
5. Kelaikan Sistem Elektronik yang digunakan.
6. Iktikad baik untuk segera memberitahukan secara tertulis kepada Pemilik Data Pribadi atas setiap kegagalan perlindungan Data Pribadi.
7. Ketersediaan aturan internal pengelolaan perlindungan Data Pribadi.
8. Tanggung jawab atas Data Pribadi yang berada dalam penguasaan Pengguna.
9. Kemudahan akses dan koreksi terhadap Data Pribadi oleh Pemilik Data Pribadi.
10. Keutuhan, akurasi, dan keabsahan serta kemutakhiran Data Pribadi.

Namun saat ini peraturan mengenai perlindungan data pribadi sudah secara terperinci diatur dalam Undang-Undang Perlindungan Data Pribadi yang disahkan

pada September 2022, yang mana sudah dirancang dari tahun 2019 oleh Kementerian Komunikasi dan Informatika Republik Indonesia. Di Undang-Undang ini mengatur bahwa tidak hanya pemerintah yang menjadi prosesor dan pengendali data pribadi namun, setiap orang hingga organisasi/institusi (Kautsar, 2023). Di Undang-Undang yang sama juga memberi pengertian terhadap data pribadi yang bersifat umum dan spesifik. Adapun data pribadi yang bersifat umum meliputi :

1. Nama lengkap
2. Jenis Kelamin
3. Kewarganegaraan
4. Agama
5. Data pribadi yang dikombinasikan untuk mengidentifikasi seseorang.

dan yang bersifat spesifik berupa :

1. Data dan informasi kesehatan
2. Data biometrik
3. Data genetika
4. Catatan kejahatan
5. Data anak
6. Data keuangan pribadi, dan
7. Data lainnya sesuai dengan ketentuan peraturan perundang-undangan.

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) adalah undang-undang yang mengatur mengenai hak dan kewajiban subjek data pribadi, pengendali data pribadi, dan prosesor data pribadi dalam

pemrosesan data pribadi, baik secara elektronik maupun nonelektronik. UU PDP bertujuan untuk melindungi data pribadi sebagai salah satu hak asasi manusia yang merupakan bagian dari pelindungan diri pribadi, sesuai dengan Undang-Undang Dasar Negara Republik Indonesia Tahun 1945. UU PDP juga dimaksudkan untuk menjamin hak warga negara atas perlindungan diri pribadi dan menumbuhkan kesadaran masyarakat serta menjamin pengakuan dan penghormatan atas pentingnya pelindungan data pribadi.

UU PDP mengatur mengenai asas, jenis, hak, pemrosesan, transfer, sanksi, kelembagaan, kerja sama internasional, partisipasi masyarakat, penyelesaian sengketa dan hukum acara, larangan, dan ketentuan pidana terkait pelindungan data pribadi. Undang-Undang bertujuan untuk mengurangi terjadinya kebocoran data masyarakat. UU PDP membuat system pemerintahan yang lebih efektif dan efesien dalam memberikan bantuan pelayanan terhadap masyarakat, Undang-Undang ini diharapkan mampu menjamin perlindungan hukum bagi data pribadi konsumen. Dalam pasal 16 ayat 2 huruf E UU PDP menyatakan Pemrosesan Data Pribadi dilakukan dengan melindungi keamanan data pribadi dari pengaksesan yang tidak sah, pengungkapan yang tidak sah, pengubahan yang tidak sah, penyalahgunaan, perusakan, dan/atau penghilangan Data Pribadi namun masih ada pasal dalam UU PDP yang belum secara jelas mengatur mengenai perlindungan data pribadi.

Contohnya pada pasal 2 ayat 2 UU PDP yang menyatakan Undang-Undang ini tidak berlaku untuk pemrosesan data pribadi oleh orang perseorangan dalam kegiatan pribadi atau rumah tangga. Pasal ini tidak jelas mengatur bagaimana batasan kegiatan pribadi atau rumah tangga yang dikecualikan dari perlindungan data pribadi. Pasal ini juga bisa menimbulkan multitafsir dalam praktiknya,

misalnya apakah data pribadi yang diproses oleh orang perseorangan untuk kepentingan bisnis atau pekerjaan masih termasuk kegiatan pribadi atau tidak.

Berdasarkan latar belakang diatas mengenai masih banyaknya hal yang perlu dianalisa dengan mendalam mengenai perlindungan hukum bagi konsumen yang mengalami kebocoran data, maka peneliti tertarik untuk melakukan penelitian yang dituangkan dengan judul **"PERLINDUNGAN HUKUM BAGI KONSUMEN TERHADAP KEBOCORAN DATA PRIBADI BERDASARKAN PASAL 16 AYAT 2 HURUF E UNDANG-UNDANG NOMOR 27 TAHUN 2022 TENTANG PERLINDUNGAN DATA PRIBADI"**

1.2 Identifikasi Masalah

Berdasarkan latar belakang di atas, maka masalah yang dapat diidentifikasi sebagi berikut :

1. Adanya peningkatan kebocoran data. Salah satu masalah utama adalah kebocoran data yang semakin meningkat di Indonesia. Kasus seperti kebocoran data di Tokopedia, registrasi SIM Card Kementerian Komunikasi dan Informatika (Kominfo), dan data pemilih dari Komisi Pemilihan Umum (KPU) menciptakan ancaman serius terhadap privasi individu dan keamanan data.
2. Adanya kebocoran data pribadi yang disebabkan peretasan atau sengaja dibocorkan oleh petugas suatu perusahaan yang mengakibatkan kerugian baik secara materiil maupun immaterial bagi konsumen, seperti pencurian identitas, dan penyalahgunaan informasi.

3. Kurangnya kesadaran dari pihak pengendali data atau pelaku usaha terkait keamanan data dari konsumen yang sangat lemah yang mengakibatkan mudahnya terjadi kebocoran data.
4. Ada beberapa faktor yang berkontribusi pada kebocoran data, termasuk kurangnya standar operasional prosedur (SOP) yang ketat, kurangnya sumber daya manusia (SDM) yang terlatih dalam keamanan data, dan kurangnya penggunaan teknologi yang aman. Semua faktor ini dapat mempermudah peretasan dan pelanggaran data.
5. Masih adanya pasal dalam Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi yang belum secara jelas mengatur mengenai perlindungan data pribadi.

1.3 Pembatasan Masalah

Berlandaskan identifikasi permasalahan yang sudah disebutkan, pembatasan masalah pada penelitian hukum ini berkaitan dengan adanya kebocoran data pribadi yang disebabkan peretasan atau sengaja dibocorkan oleh petugas suatu perusahaan yang mengakibatkan kerugian baik secara materiil maupun immaterial bagi konsumen, seperti pencurian identitas, dan penyalahgunaan informasi. Pembantasan masalah selanjutnya adalah masih adanya pasal dalam Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi yang belum secara jelas mengatur mengenai perlindungan data pribadi.

1.4 Rumusan Masalah

Berdasarkan latar belakang tersebut, maka permasalahan yang akan dikaji dalam penelitian ini adalah :

1. Bagaimana perlindungan hukum terhadap konsumen terkait kebocoran data pribadi dalam prespektif perbandingan?
2. Bagaimana upaya hukum bagi konsumen yang mengalami kerugian akibat kebocoran data pribadi?

1.5 Tujuan Penulisan

Berdasarkan permasalahan diatas, maka adapun tujuan penelitian adalah sebagai berikut :

1. Tujuan Umum

Adapun tujuan umum yang ingin dicapai dalam penulisan karya akhir ini yaitu:

a. Untuk menambah wawasan pada bidang keperdataan mengenai bagaiman perlindungan hukum terhadap konsumen terkait kebocoran data pribadi dalam prespektif perbandingan.
b. Untuk menambah wawasan mengenai bagaimana upaya hukum bagi konsumen yang mengalami kerugian akibat kebocoran data pribadi.

2. Tujuan Khusus

Adapun tujuan khusus yang ingin dicapai dalam penulisan proposal ini yaitu:

a. Untuk mengetahui bagaiman perlindungan hukum terhadap konsumen terkait kebocoran data pribadi dalam prespektif perbandingan.
b. Untuk mengetahui bagaiman upaya hukum bagi konsumen yang mengalami kerugian akibat kebocoran data pribadi.

1.6 Manfaat Penulisan

Adapun manfaat yang diharapkan oleh penulis dalam karya tulis ini adalah sebagai berikut :

1. Manfaat Teoritis :

   Hasil penelitian ini secara akademis diharapkan mampu memberikan kontribusi pemikiran sehingga menambah wawasan dalam proses pengembangan ilmu pengetahuan khususnya pada bidang Ilmu Hukum Perdata dan dapat juga memberikan kontribusi terkait pembahasan mengenai Perlindungan Hukum Bagi Konsumen Terhadap Kebocoran Data Pribadi Berdasarkan Pasal 16 Ayat 2 Huruf E Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi.
2. Manfaat Praktis :
   a. Bagi masyarakat, penelitian ini dapat memberikan informasi dan pemahaman bagi konsumen tentang hak dan kewajiban mereka dalam menghadapi kebocoran data, serta cara-cara untuk melindungi diri dan menyelesaikan sengketa yang timbul akibat kebocoran data tersebut.
   b. Bagi pengendali data, penelitian ini dapat meningkatkan kesadaran dan tanggung jawab dari pengendali data untuk menghindari terjadinya kebocoran data dan memberikan jaminan keamanan data kepada konsumen.
   c. Bagi penulis, penelitian ini merupakan salah satu syarat untuk dapat menyelesaikan Sarjana Strata I di Fakultas Hukum dan Ilmu Sosial Prodi Ilmu Hukum Universitas Pendidikan Ganesha khususnya pada bagian Ilmu Hukum Keperdataan.