BAB I

PENDAHULUAN

A. Latar Belakang Masalah

Hakikat negara Indonesia sebagai negara hukum yang termaktub dalam Pasal 1 Ayat (3) Undang Undang Dasar Negara Republik Indonesia Tahun 1945 (selanjutnya disebut UUD NRI Tahun 1945). Hal ini berlandaskan pada konsep teori kedaulatan negara yang pada pokoknya menyatakan bahwa kekuasaan tertinggi dalam suatu negara adalah hukum, oleh karena itu semua lembaga negara termasuk rakyatnya wajib menaati, menaati, dan menegakkan hukum tersebut dengan tidak ada kecualinya.[1]

Dapat dikatakan bahwa saat ini manusia menjalani kehidupan yang tidak dapat dipisahkan dari perkembangan teknologi dalam segala aktivitasnya, terutama pesatnya perkembangan teknologi informasi dan komunikasi di masyarakat. Hampir seluruh aspek kehidupan mengalami perkembangan, baik ekonomi, sosial, maupun budaya. Di era globalisasi yang semakin pesat ini, pesatnya perkembangan teknologi telah membawa kemajuan di berbagai bidang dan membawa banyak manfaat. Dalam kehidupan, manusia dituntut untuk memanfaatkan teknologi untuk mempermudah pekerjaannya. Pengembangan sumber daya manusia juga sangat dibutuhkan dalam

[1] B. Hestu Cipto Handoyo, *Hukum Tata Negara, Kewarganegaraan dan Hak Asasi Manusia, Memahami Proses Konsolidasi Sistem Demokrasi di Indonesia*, (Yogyakarta: Universitas Atma Jaya Press, 2003); hal. 12.

perkembangan teknologi. Kemajuan teknologi dan informasi akan memberikan dampak yang signifikan terhadap perkembangan masyarakat.

Perkembangan teknologi informasi dan komunikasi selama beberapa dekade ini telah membawa perubahan dan tantangan dalam hal perlindungan privasi individu maupun organisasi. Kemajuan digitalisasi memungkinkan individu maupun organisasi untuk melakukan inovasi-inovasi baru dalam pengolahan informasi, termasuk data. Dengan kemajuan digitalisasi dan teknologi informasi serta komunikasi, terdapat beberapa kasus di mana informasi yang seharusnya tidak boleh dipublikasikan justru dipublikasikan tanpa sepengetahuan dan persetujuan pihak-pihak yang terlibat, sehingga dapat menimbulkan penyalahgunaan dan kebocoran data. Apalagi jika informasi yang dipublikasikan tersebut merupakan data pribadi, niscaya akan menimbulkan kerugian bagi pihak-pihak yang terlibat.

Secara umum, data pribadi adalah data yang memberikan informasi yang dapat mengidentifikasi seseorang, seperti nama, usia, jenis kelamin, latar belakang pendidikan, pekerjaan, dan alamat, dan diperlakukan sebagai informasi rahasia. Data yang dapat digunakan untuk mengidentifikasi seseorang dengan menggabungkan berbagai informasi tersebut juga termasuk dalam data pribadi. Hal ini meliputi kode-kode, angka, simbol, huruf, dan sebagainya yang berfungsi sebagai kriteria untuk menunjukkan karakteristik seseorang.[2]

[2] https://vida.id/id/blog/data-pribadi, diakses pada tanggal 30 Mei 2025.

Data pribadi harus dijaga dengan baik karena penyalahgunaan data pribadi akan mengakibatkan kerugian baik materiil maupun non materiil, tidak hanya bagi orang yang menjadi subjek data pribadi, tetapi juga bagi organisasi yang mengolah data pribadi. Setiap orang mempunyai hak asasi manusia, termasuk hak atas privasi dan merupakan hak asasi individu yang secara kodrati dilindungi oleh negara. Begitu pula setiap warga negara mempunyai hak konstitusional sebagaimana diatur dalam UUD NRI Tahun 1945. Pasal 28G Ayat (1) UUD NRI Tahun 1945 menyatakan bahwa "Setiap orang berhak melindungi diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya serta berhak atas rasa aman dan tenteram dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu." Dalam pasal ini, dengan berkembangnya teknologi informasi dan komunikasi, dapat disimpulkan bahwa hak yang dimiliki oleh setiap individu adalah hak atas privasi.[3]

Data pribadi menjadi suatu aset yang bernilai ekonomis sangat tinggi di era big data, sehingga rentan untuk menjadi objek kesewenangan, demi keuntungan semata pihak lain. Tindakan tersebut bertujuan untuk mencari keuntungan dari penyalahgunaan data pribadi mencakup rangkaian proses mencuri, menyebarkan, menjual, dan menggunakan data yang bukan miliknya. Tidak hanya itu, aksi perundungan, pemberian ancaman,

[3] Pasal 28G Ayat (1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945

penipuan, hingga pembobolan akun menjadi sesuatu yang tidak bisa dihindarkan dalam dunia digital.[4]

Menurut data dari databoks pada kuartal III tahun 2022, Indonesia menduduki peringkat ke-3 sebagai negara dengan kasus kebocoran data terbanyak di dunia. Pada kuartal tersebut, Indonesia mengalami kebocoran data sebanyak 12.742.031 akun. Jumlah kebocoran data tersebut bisa dibilang sangat besar dan memalukan bagi negara Indonesia.[5]

Kebocoran data merupakan sebuah pengungkapan informasi yang bersifat rahasia baik disengaja *(intentional threats)* maupun tidak disengaja *(inadvertent threats)* kepada pihak yang tidak berwenang.[6]

Sebagai contoh, pada September 2022 terjadi kebocoran data registrasi *SIM Card* berupa nama operator, nomor ponsel, Nomor Induk Kependudukan (NIK) yang digunakan untuk transaksi jual beli data pribadi di pasar gelap (*black market*). Kebocoran data tersebut diketahui publik melalui cuitan berupa tangkapan layar yang menunjukkan informasi tentang tawaran penjualan data untuk 1,3 miliar pengguna kartu SIM. Data tersebut dijual oleh akun bernama Bjorka dengan menjual data sebesar 87 GB senilai US$ 50.000 atau setara dengan 745 juta rupiah (asumsi US$ 1 = Rp 14.900).

---

[4] Muhammad Fikri, Shelvi Rusdiana, *Ruang Lingkup Perlindungan Data Pribadi: Kajian Hukum Posistif Indonesia, Ganesha Law Review*, Vol.5, No.1, 2023, hal.41

[5] Kasus Kebocoran Data di Indonesia Melonjak 143% pada Kuartal II 2022, diakses pada tanggal 5 Juni 2025.

[6] Delpiero, M., Reynaldi, F. A., Ningdiah, I. U., Muthmainnah, N, *Analisis yuridis kebijakan privasi dan pertanggungjawaban online marketplace dalam perlindungan data pribadi pengguna pada kasus kebocoran data, Padjadjaran Law Review*, Vol.9, No.1, 2021, hal.221

Kebocoran data ini merugikan para pengguna *SIM Card* karena datanya digunakan untuk kegiatan yang dapat berujung pada perbuatan kriminal.[7]

Data mengejutkan ini diperoleh Bjorka berdasarkan hasil kajian kebijakan Kominfo terkait kewajiban registrasi kartu perdana prabayar dengan NIK dan Kartu Keluarga (KK) pada 31 Oktober 2017. Bjorka telah menyusun kebijakan lengkap terkait kebijakan dimaksud, yakni nomor telepon seluler yang dimaksud dapat diblokir apabila melebihi batas waktu yang ditentukan. Di era digital, kemungkinan kebocoran data tidak dapat dihindari, dan dengan begitu banyak data yang disimpan dalam bentuk digital, nilai data pribadi juga meningkat, menciptakan insentif finansial yang semakin besar bagi penjahat digital.[8]

Kementerian Komunikasi dan Informatika (Selanjutnya disebut Kominfo) membenarkan telah melakukan investigasi internal terkait dugaan kebocoran data tersebut. Kominfo membantah kebocoran data kartu SIM tersebut bersumber dari internal dan juga membantah klaim kebocoran tersebut berasal dari internal kementerian. Pakar keamanan siber yang juga Ketua Pusat Penelitian Keamanan Sistem Komunikasi dan Informasi (CISSReC) Pratama Persada menjelaskan kebocoran tersebut diunggah pada Selasa sore, 31 Agustus oleh salah seorang anggota situs *forum broked.to* dengan ID "Bjorka" yang sebelumnya juga pernah membocorkan data riwayat pelanggan Indihome. Menurut Pratama, data pastinya adalah

[7] https://www.pinterpolitik.com/in-depth/sim-card-bocor-kominfo-bersalah/, diakses pada tanggal 5 Juni 2025.
[8] Ibid.

1.304.401.300 baris dengan total ukuran 87 GB. Sampel data tersebut dicek dengan memanggil nomor acak dan semua nomor masih aktif, artinya dari 1,5 juta sampel data yang diberikan, data tersebut valid.[9]

Sehubungan dengan kasus kebocoran data pribadi di atas, Kementerian Komunikasi dan Digital Republik Indonesia (Selanjutnya disebut Komdigi) memiliki tanggung jawab yang signifikan terkait perlindungan data pribadi. Komdigi bertanggung jawab untuk perumusan kebijakan, pengawasan dan penegakan hukum dan pendidikan dan sosialisasi. Adapun konsekuensi hukum terkait pertanggungjawaban Komdigi atas kebocoran data pribadi meliputi sanksi administratif, termasuk denda dan pencabutan izin usaha, bagi penyelenggara sistem elektronik yang tidak mematuhi ketentuan. Perorangan juga dapat mengajukan gugatan hukum terhadap penyelenggara yang melanggar haknya. Pelanggaran hubungan kepercayaan dapat mengakibatkan hilangnya kredibilitas sosial, merugikan Kementerian Komunikasi dan Digital serta penyelenggara sistem elektronik, dan pada akhirnya memengaruhi layanan digital di Indonesia.

Baik informasi tersebut berasal dari Komdigi atau bukan, pemerintah seharusnya dapat memberikan pengawasan dan keamanan kepada perusahaan utilitas yang mengalami kebocoran data. Hal ini sesuai dengan pandangan *Alan R. Coffey* bahwa strategi pencegahan kejahatan dapat

---

[9] https://www.kompas.com/tren/read/2022/09/02/083741365/ramai-soal-dugaan-13-miliar-data-sim-card-bocor-ini-analisis-pakar?page=all#page2, diakses pada tanggal 5 Juni 2025.

dilaksanakan melalui dua fokus utama yaitu mencegah terjadinya kebocoran awal dan mencegah terjadinya kebocoran dan kejahatan.[10]

Kasus kebocoran data yang kerap kali terjadi mengindikasikan sistem keamanan data yang belum dibangun dengan baik. Hal ini terjadi pada instansi baik publik maupun privat yang memiliki bank data, tidak mempunyai server yang cukup baik untuk melindungi data tersebut. Sistem keamanan data mencakup server atau domain yang diterapkan dalam sistem penyimpanan data maupun sumber daya manusia yang membuat dan menjalankannya. Server ataupun domain yang ada saat ini dianggap masih lemah, terlebih sumber daya manusia yang membangun dan menjalankan sistem keamanan data belum mempunyai kualitas dan kesadaran terkait perlindungan data pribadi, baik secara personal maupun penguatan SDM secara kelembagaan.[11]

Kebocoran data pribadi menurut UU No. 27 Tahun 2022 Tentang PDP disebut dengan istilah kegagalan perlindungan data pribadi, yaitu kegagalan melindungi data pribadi individu dalam hal kerahasiaan, integritas, dan ketersediaan data tersebut, termasuk setiap pelanggaran keamanan yang secara sengaja atau tidak sengaja mengakibatkan penghancuran, kehilangan, pengubahan, pengungkapan, atau akses tidak sah terhadap data pribadi yang dikirimkan, disimpan, atau diproses.[12]

---

[10] https://www.pinterpolitik.com/in-depth/sim-card-bocor-kominfo-bersalah/, diakses pada tanggal 5 Juni 2025.

[11] Ibid, hal.87

[12] Pasal 46 Ayat (1) Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi

Berdasarkan ketentuan Pasal 1 Angka 4 UU No. 27 Tahun 2022 Tentang PDP, Komdigi tergolong sebagai pengendali data pribadi yang berbentuk badan publik yang tunduk pada UU No. 27 Tahun 2022 Tentang PDP. Pengendali data pribadi adalah orang perseorangan, badan publik, atau organisasi internasional yang bertindak sendiri atau bersama-sama dalam mengolah data pribadi atas nama pengendali data pribadi.[13]

Badan publik adalah badan eksekutif, legislatif, yudikatif, dan badan lain yang tugas dan fungsinya yang utama berkaitan dengan penyelenggaraan negara dan yang sebagian atau seluruh dananya bersumber dari APBN dan/atau APBD atau lembaga swadaya masyarakat yang sebagian atau seluruh dananya bersumber dari APBN dan/atau APBD, sumbangan masyarakat, dan/atau luar negeri.[14]

Tujuan utama UU No. 27 Tahun 2022 Tentang PDP adalah untuk melindungi Hak Asasi Manusia. Undang-Undang ini bertujuan untuk menjaga hak asasi manusia dalam konteks perlindungan individu, termasuk data pribadi, serta untuk memastikan hak warga negara dalam mendapatkan perlindungan atas data pribadi mereka. Selain itu, Undang-Undang ini juga berupaya meningkatkan kesadaran masyarakat mengenai pentingnya perlindungan data pribadi. Pasal 16 Ayat (2) huruf e UU No. 27 Tahun 2022 Tentang PDP mengatur bahwa pengendali data pribadi berkewajiban untuk melindungi keamanan data pribadi terhadap akses yang tidak sah,

[13] Pasal 1 Ayat 4 Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi

[14] Pasal 1 Ayat 9 Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi

pengungkapan, penggunaan yang tidak sah, penghancuran, kehilangan, dan untuk mencegah kebocoran data pribadi.[15]

Selanjutnya Pasal 46 Ayat (1) UU No. 27 Tahun 2022 Tentang PDP mengatur bahwa dalam hal terjadinya pelanggaran data pribadi, pengendali data pribadi wajib memberikan pemberitahuan tertulis kepada pengguna (subjek data pribadi) dan lembaga yang mengendalikan data pribadi dalam waktu 3x24 jam.[16] Apabila kebocoran informasi pribadi tersebut mengganggu pelayanan publik atau berdampak signifikan terhadap kepentingan masyarakat setempat, maka pemerintah (dalam hal ini Kementerian Komunikasi dan Digital) wajib mengumumkan kegagalan perlindungan data pribadi.

Kebocoran data pribadi tentu akan berdampak serius terhadap subjek data pribadi yang data pribadinya tersebar luas. Selain privasinya terganggu, mereka dapat menjadi korban kejahatan siber, seperti pemalsuan, penipuan, pemerasan, atau praktik *doxing*, yaitu membongkar dan menyebarkan informasi target sasaran oleh pihak-pihak yang tidak berwenang.[17]

Sebagaimana Pasal 65 Ayat (1) UU No. 27 Tahun 2022 Tentang PDP mengatur bahwa setiap orang dilarang secara melawan hukum memperoleh atau mengumpulkan Data Pribadi yang bukan miliknya dengan maksud

---

[15] Pasal 16 Ayat (2) huruf e Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi

[16] Pasal 46 Ayat (1) huruf e Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi

[17] Oktaviani, S., Dewata, Y. J., & Fadlian, A, *Pertanggung Jawaban Pidana Kebocoran Data BPJS dalam Perspektif UU ITE, De Juncto Delicti: Journal Of Law*, Vol.1, No.2, 2021, hal.153

untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian Subjek Data Pribadi.[18]

Sebelum disahkannya Undang-Undang Nomor 27 Tahun 2022 pengaturan terkait perlindungan data pribadi masih bersifat parsial dan belum komprehensif. Salah satu regulasi yang mengatur hal tersebut adalah Undang-Undang Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik (Selanjutnya disebut UU No.1 Tahun 2024 Tentang ITE). Regulasi ini memang telah mengatur terkait perlindungan data pribadi akan tetapi, masih belum lengkap dan komprehensif. UU No.1 Tahun 2024 Tentang ITE memang telah diatur perbuatan yang dilarang menyangkut data pribadi akan tetapi, yang menjadi permasalahan adalah dalam UU No.1 Tahun 2024 Tentang ITE tidak diatur mengenai definisi data pribadi secara jelas. Oleh karena itu, jika memakai Undang-Undang ini dalam mengajukan gugatan jika terjadi perselisihan atau tindak pidana maka penggugat atau pelapor akan mengalami kesulitan dalam hal pembuktian. Atas hal tersebut maka diperlukan regulasi yang mengatur secara komprehensif terkait perlindungan data pribadi.[19]

Selain diatur dalam UU No. 27 Tahun 2022 Tentang PDP, kebocoran data pribadi yang diselenggarakan oleh pemerintah juga diatur di dalam

---

[18] Pasal 65 Ayat (1) Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi

[19] Dade, L. L., Waha, C. J., Nachrawy, N., *Kajian Yuridis Tentang Tindak Pidana Penyebaran Data Pribadi Melalui Internet (Doxing) Di Indonesia. LEX PRIVATUM*, Vol.13, No.3, 2024, hal.5

Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik (selanjutnya disebut PP No. 71 Tahun 2019 Tentang PSTE). Dalam Pasal 14 Ayat (5) PP No. 71 Tahun 2019 Tentang PSTE diatur bahwa dalam hal terjadi kebocoran data pribadi yang dikendalikan (kegagalan perlindungan data pribadi), penyelenggara sistem elektronik (yang dalam hal ini termasuk pemerintah) berkewajiban memberitahukan secara tertulis kepada pemegang data pribadi.[20] Dapat disimpulkan bahwa Pemerintah atau penyelenggara negara dalam PP No. 71 Tahun 2019 Tentang PSTE tergolong sebagai penyelenggara sistem elektronik lingkup publik.

Pemberitahuan secara tertulis apabila terjadi kegagalan pelindungan rahasia data pribadi tersebut harus memenuhi ketentuan dalam Pasal 28 Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 20 Tahun 2016 Tentang Perlindungan Data Pribadi Dalam Sistem Elektronik (selanjutnya disebut Perkominfo No. 20 Tahun 2016 Tentang PDP Dalam Sistem Elektronik). Pasal 100 Perkominfo No. 20 Tahun 2016 Tentang PDP Dalam Sistem Elektronik juga mengatur bahwa apabila penyelenggara sistem elektronik tidak memberitahukan secara tertulis kepada yang bersangkutan, maka dapat dikenakan sanksi administratif berupa teguran tertulis, sanksi administratif, penghentian sementara, penghentian akses, atau pencabutan izin dan sebagainya. Sanksi

[20] Pasal 14 Ayat (5) Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik

administratif tersebut dilaksanakan oleh Menteri yang menyelenggarakan urusan pemerintahan di bidang komunikasi dan informatika.[21]

PP No. 71 Tahun 2019 Tentang PSTE dan Perkominfo No. 20 Tahun 2016 Tentang PDP Dalam Sistem Elektronik mengatur bahwa kedua peraturan tersebut juga mengatur apa yang harus dilakukan jika ada kebocoran data pribadi, yang berlaku untuk swasta maupun badan publik (penyelenggara negara). Selain tanggung jawab pemerintah selaku pengendali data pribadi untuk melakukan pemberitahuan tertulis jika ada kebocoran data pribadi, Pasal 12 UU No. 27 Tahun 2022 Tentang PDP menegaskan bahwa subjek data pribadi berhak menggugat dan menerima ganti rugi atas pelanggaran pemrosesan data pribadi tentang dirinya sesuai dengan ketentuan peraturan perundang-undangan.[22]

Pengaturan mengenai pelindungan data pribadi sebelum berlakunya UU No. 27 Tahun 2022 tentang PDP dapat ditemukan dalam beberapa peraturan perundang-undangan, walaupun tidak secara spesifik mengatur pelindungan data pribadi, tetapi berguna dalam rangka meningkatkan efektivitas dalam pelaksanaan pelindungan data pribadi.[23]

Berangkat dari ketidakefektivitas tersebut, regulasi pelindungan data pribadi yang diatur di peraturan perundang-undangan sebelumnya, maka

---

[21] Pasal 28 Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 20 Tahun 2016 Tentang Perlindungan Data Pribadi Dalam Sistem Elektronik

[22] Pasal 12 Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi

[23] Ngompat, Y. L., *Ketidaksetaraan Sanksi Dalam Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi Doctoral dissertation*, Universitas Atma Jaya Yogyakarta, 2023, hal.20

lembaga legislatif mengesahkan regulasi yang secara spesifik dan komprhensif mengatur mengenai data pribadi yaitu UU No. 27 Tahun 2022 tentang PDP. Pengesahan UU No. 27 Tahun 2022 tentang PDP merupakan jawaban atas kekosongan hukum dalam memproteksi keamanan data pribadi dan dapat menjadi landasan dalam menindak berbagai kejahatan yang berhubungan dengan data pribadi. Berbagai aturan sebelumnya mengatur mengenai data pribadi namun tidak secara spesifik dijelaskan, sehingga dibentuknya UU No. 27 Tahun 2022 bertujuan untuk melindungi berbagai kepentingan individu berkaitan dengan data pribadinya serta hukuman atau sanksi terhadap pelaku yang melakukan pelanggaran terhadap data pribadi.[24]

Di era digital, perlindungan data pribadi bukan hanya menjadi tanggung jawab individu, tetapi juga perusahaan dan penyedia layanan yang mengelola data tersebut. Namun, sebagai pengguna, masyarakat harus selalu mengambil tindakan proaktif untuk melindungi data pribadi dari ancaman kejahatan dunia maya. Dengan memahami ancaman yang ada dan mengambil tindakan pencegahan, maka dapat meminimalkan risiko penyalahgunaan data pribadi dan menjaga privasi serta keamanan dalam kehidupan digital. Semuel menjabarkan 5 (lima) alasan utama pentingnya menjaga data pribadi yaitu sebagai berikut :[25]

[24] Ibid.
[25] https://www.kominfo.go.id/content/detail/19991/5-alasan-mengapa-data-pribadi-perlu-dilindungi/0/sorotan_media, diakses pada tanggal 30 Mei 2025.

1. Intimidasi *online* terkait gender. Semuel menyebutkan bahwa data pribadi berupa jenis kelamin patut dilindungi untuk menghindari kasus pelecehan seksual atau perundungan (*bullying*) secara *online*;
2. Mencegah penyalahgunaan data pribadi oleh pihak yang tidak bertanggung jawab;
3. Menjauhi potensi penipuan;
4. Menghindari potensi pencemaran nama baik; dan
5. Hak kendali atas data pribadi.

Data pribadi merupakan aset yang paling berharga bagi setiap individu. Kebocoran data pribadi mempunyai dampak buruk yang serius terhadap seseorang yang data pribadinya tersebar luas. Pencurian, penjualan, dan penyalahgunaan data pribadi masyarakat merupakan pelanggaran hukum.[26]

Berdasarkan uraian di atas, penulis tertarik untuk melakukan penelitian lebih lanjut dalam bentuk skripsi yang berjudul **"TINJAUAN YURIDIS TENTANG KEBOCORAN DATA *SUBSCRIBER IDENTITY MODULE* YANG DIRETAS DARI KEMENTRIAN KOMUNIKASI DAN DIGITAL."**

B. Identifikasi dan Perumusan Masalah

Berdasarkan latar belakang tersebut, maka dapat diambil beberapa masalah yang akan dibahas yaitu :

[26] Bahtiar Naylawati, *Darurat Kebocoran Data: Kebuntuan Regulasi Pemerintah, Development Policy and Management Review (DPMR)*, 2024, hal.100.

1. Bagaimana mekanisme penegakan hukum tentang penjualan data *Subscriber Identity Module* yang mengakibatkan kerugian bagi subjek data pribadi ?
2. Bagaimana bentuk pertanggungjawaban Kementerian Komunikasi dan Digital dalam melindungi data *Subscriber Identity Module*?

C. Tujuan Penelitian

Berdasarkan rumusan masalah diatas, adapun yang menjadi tujuan dari penelitian ini yaitu :

1. Mengetahui mekanisme penegakan hukum terkait dengan penjualan data *Subscriber Identity Module* yang berakibat pada kerugian bagi subjek data pribadi dengan fokus pada peraturan perundang-undangan yang berlaku.
2. Mengetahui bagaimana bentuk tanggungjawab hukum Kementrian Komunikasi dan Digital dalam melindungi data *Subscriber Identity Module*.

D. Kegunaan Penelitian

Dalam suatu penelitian tentu memiliki kegunaan yang bernilai serta bermanfaat, terutama bagi pembaca. Adapun kegunaan dalam penelitian ini yaitu:

a) Akademis

Penelitian ini diharapkan dapat memberikan pemahaman yang lebih mendalam mengenai aspek yuridis dari kebocoran data pribadi. Selain itu, penelitian ini diharapkan dapat memperluas wawasan

akademis mengenai tanggung jawab negara, khususnya kementerian atau lembaga pemerintah, dalam menjamin perlindungan data pribadi warga negara, dan penelitian ini diharapkan menjadi referensi ilmiah dan sumber informasi hukum yang relevan dalam kajian akademik.

b) Kelembagaan

Penelitian ini dapat menjadi bahan evaluasi dan pertimbangan dalam pembentukan, penyempurnaan, serta pelaksanaan kebijakan perlindungan data pribadi, khususnya menyangkut sistem keamanan data digital di lingkungan instansi pemerintah. Hasil kajian ini diharapkan membantu dalam mencegah terulangnya insiden kebocoran data serupa di masa mendatang.

c) Sosial

Penelitian ini memberikan edukasi hukum kepada masyarakat agar lebih memahami pentingnya perlindungan data pribadi serta hak-hak hukum yang dimiliki apabila terjadi pelanggaran terhadap data pribadinya. Dengan demikian, masyarakat diharapkan menjadi lebih kritis dan berhati-hati dalam mengelola data pribadinya di era digital.