BAB I
PENDAHULUAN

A. Latar Belakang

Jenis tindak pidana mayantara (*cyber crime*) merupakan tindak pidana yang timbul karena dampak globalisasi. Globalisasi sangat dipengaruhi oleh perkembangan Teknologi Informasi dan Komunikasi (TIK) yang semakin pesat dan canggih. Perkembangan TIK selain menghadirkan dampak positif dan juga memiliki dampak negatif. Dampak positif dan negatif dari perkembangan TIK layaknya dua sisi koin yang harus dibedakan namun tidak dapat dipisahkan. Maknanya terhadap sisi positif, tentu dapat dimanfaatkan untuk melakukan pembangunan dan mencapai tujuan nasional yang dicita-citakan oleh bangsa Indonesia[1].

Sudut pandang dari sisi negatifnya, yaitu adanya globalisasi kejahatan dan meningkatnya kuantitas serta kualitas (modus operandi) tindak pidana. Dengan perkembangan TIK, tindak pidana antar negara bahkan antar benua dapat terjadi dengan mudah, karena TIK mampu meniadakan jarak atau sekat-sekat wilayah suatu negara dengan negara lain. Bisa saja pelaku tindak pidana mayantara melangsungkan operandinya di Indonesia meskipun sedang berada di luar Indonesia dengan dukungan jaringan internet.

[1] Kristian dan Yopi Gunawan, *Sekelumit tentang Penyadapan dalam Hukum Positif di Indonesia* (Bandung: Nuansa Aulia, 2013), Hal 4.

Masa Pandemi Covid-19 saat ini yang membatasi kegiatan penduduk di luar rumah berdampak meningkatnya penggunaan internet, mulai dari kegiatan *e-commerse*, *e-learning*, pelayanan publik dan lain sebagainya. Pandemi COVID-19 telah mengubah perilaku masyarakat secara masif, dari yang semula konvensional banyak yang dialihkan menjadi digital. Hasil Survei Asosiasi Pengguna Jaringan Internet Indonesia (APJII) tahun 2020 menunjukkan, pengguna internet di Indonesia mencapai 196 juta penduduk atau 73,7 persen. Angka tersebut naik 8,9 persen jika dibandingkan sebelum pandemi pada 2018 lalu yang hanya sekitar 64,8 persen pengguna internet di Indonesia[2]. Kemudian kembali mengalami kenaikan di tahun 2021 sebesar 77,02 persen.

Kenaikan signifikan pengguna internet pada masa pandemi ini, menjadi salah satu faktor penyebab meningkatnya kejahatan di mayantara, salah satunya pencurian data pribadi pengguna internet. Tercatat di dalam laporan tahunan Badan Siber dan Sandi Negara (BSSN) pada tahun 2020 telah terjadi kebocoran data sebanyak 91 juta pengguna situs belanja online Tokopedia, yang tidak lama kemudian disusul oleh kebocoran data 1,2 juta pengguna situs Bhinneka. Selain kasus tersebut, pada pertengahan 2020 di masa pemilihan umum, adanya akun yang mengakui telah membobol 2,3 juta data warga Indonesia dari Komisi Pemilihan Umum (KPU)[3].

Modus pencurian data pribadi dari sejumlah sistem elektronik tersebut diatas terjadi karena adanya akses ilegal pelaku dengan menggunakan *malware* pencuri

[2] Buletin APJII Edisi 79 bulan Januari 2021, diakses melalui web https://apjii.or.id/ pada 12 Oktober 2021.

[3] Laporan Tahunan Monitoring Keamanan Siber BSSN Tahun 2020, Hal 11.

data. Menurut laporan yang dirilis BSSN di tahun 2020, top 5 *malware* pencuri data yang digunakan pelaku meliputi: njRAT, Emotet, Wacatac, PuffStealer, dan AZORuit. Cara kerja *malware* pencuri data tersebut yaitu melalui *Exploit Kit* dan *spam email* yang berkedok *invoice* palsu. Ketika pengguna membuka atau mengunduh kiriman tersebut secara tidak sadar pengguna mengeksekusi malware tersebut. Kemudian setelah itu komputer yang terinfeksi akan terhubung dengaan server penyerang (C2 server) untuk menerima dan mengirim pesan, sehingga pelaku dapat mengakses data pribadi pengguna yang seharusnya tersimpan secara aman[4].

Dari sekian kasus pencurian data pribadi pengguna sistem elektronik tersebut diatas, belum ada satupun pelaku yang ditangkap dan diproses hukum. Hal ini tentunya dipengaruhi oleh beberapa faktor yang menurut penulis sangat menarik untuk diteliti dalam proposal skripsi ini. Menurut dugaan awal penulis, belum optimalnya penegakan hukum mengenai pencurian data pribadi melalui sistem elektronik disebabkan karena pelaku menggunakan teknologi canggih untuk menjalankan operandinya, sehingga penegak hukum kesulitan dalam mengungkap kasus tersebut. Selain itu, norma hukum yang mengatur tentang perlindungan data pribadi pengguna sistem elektronik juga masih samar dan belum lengkap.

Pada umumnya, pelaku pencurian data pribadi pengguna sistem elektronik dilakukan dengan teknik peretasan (*hacking*) yaitu dengan meretas atau masuk secara ilegel kedalam database sistem elektronik. Setelah mendapatkan data pribadi berupa *username*, NIP, nomor kartu keluarga, tempat dan tanggal lahir, nomor HP,

[4] *Ibid*., Hal. 40.

hingga nama-nama anggota keluarga pengguna sistem elektronik, kemudian dijual belikan oleh pelaku di *online marketplace*. Tindakan jual beli data pribadi sangat rentan disalahgunakan untuk tindakan-tindakan lain yang dapat merugikan pemilik data pribadi tersebut.

Menurut hasil penelitian yang dilakukan oleh Sahat Maruli Tua Situmeang, 2021, implementasi dari kebijakan hukum perlindungan data saat ini dinilai belum berjalan dengan baik. Dalam konsep pengaturan perlindungan data pribadi diharapkan adanya aturan yang lebih tegas dan komprehensif dan sesuai dengan perkembangan sosial budaya, ekonomi serta politik serta menjungjung tinggi nilai-nilai atau norma, etika dan kesusilaan serta agama, dengan harapan hukum tidak ketinggalan dengan perkembangan teknologi dan informasi[5].

Terlepas belum lengkapnya pengaturan mengenai perlindungan data pribadi pengguna sistem elektronik, saat ini yang dapat menjadi alternatif untuk perlindungan hukum yaitu Pasal 26 Undang-Undang Nomor 9 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 dan Pasal 30 Ayat (2) *jo* Pasal 46 Ayat (2) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Selain pengaturan yang ada di dalam UU ITE, juga diatur di dalam Peraturan Pemerintah Nomr 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE). PP PSTE mengatur mengenai kewajiban-kewajiban bagi penyelenggaran sistem elektronik untuk memastikan data pribadi pengguna harus dikelola dan diamankan dengan baik dan apabila melanggar

[5] Sahat Maruli Tua Situmeang, 2021, *Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna Dalam Perspektif Hukum Siber*, Bandung: SASI Volume 27 Nomor 1, Januari-Maret 2021, Hal. 38-52.

kewajiban-kewajiban tersebut akan dikenakan sanksi administratif berupa teguran tertulis, denda administratif, penghentian sementara, pemutusan Akses, dan/atau dikeluarkan dari daftar[6]. Namun kenyataannya sebagaimana uraian calon peneliti tersebut di atas, bahwa selama ini praktik-praktik pencurian yang diteruskan dengan perbuatan penyalahgunaan data pribadi dengan cara diperjualbelikan secara ilegal banyak terjadi.

Berdasarkan uraian diatas, penulis menilai sangat penting untuk membahas alternatif perlindungan hukum pemilik data pribadi dan pemilik sistem elektronik apabila data pribadi yang disimpan di dalam sistem elektronik dicuri dan disalahgunakan oleh pelaku yang tidak bertanggung jawab dengan menulis skripsi yang berjudul ANALISIS YURIDIS PERLINDUNGAN KORBAN TINDAK PIDANA PENCURIAN DATA PRIBADI MELALUI SISTEM ELEKTRONIK.

B. Rumusan Masalah

Berdasarkan latar belakang masalah yang telah diuraikan di atas, maka rumusan masalahnya dapat ditetapkan sebagai berikut :

1. Bagaimana modus terjadinya pencurian data pribadi melalui sistem elektronik?
2. Apa sajakah bentuk-bentuk perlindungan hukum bagi korban tindak pidana pencurian data pribadi dalam hukum positif Indonesia?
3. Bagaimana implementasi atau penerapan perlindungan hukum terhadap korban tindak pidana pencurian data pribadi?

[6] Pasal 100 Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

C. Tujuan Penulisan

Tujuan disusunnya skripsi ini yaitu:

1. Untuk memberikan pemahaman terkait modus terjadinya pencurian data pribadi melalui sistem elektronik;
2. Untuk memberikan informasi dan pemahaman terkait bentuk-bentuk perlindungan hukum bagi korban tindak pidana pencurian data pribadi dalam hukum positif Indonesia;
3. Untuk memberikan pemahaman terkait implementasi atau penerapan perlindungan hukum terhadap korban tindak pidana pencurian data pribadi.

D. Manfaat Penulisan

Adapun manfaat disusunnya skripsi ini yaitu:

1. Manfaat Teoritis
    a. Hasil penulisan ini diharapkan dapat memberikan masukan positif bagi perkembangan ilmu hukum, khususnya dalam bidang ilmu hukum pidana mengenai penerapan perlindungan korban pencurian data.
    b. Hasil penulisan ini diharapkan dapat memberikan referensi dalam bidang akademis dan sebagai kepustakaan hukum pidana.
2. Manfaat Praktis
    a. Pihak yang melindungi korban

Hasil penulisan ini diharapkan dapat dijadikan suatu pandangan atau langkah ke depan yang positif terhadap pelaksanaan perlindungan hukum bagi korban pencurian data pribadi.

b. Korban

Hasil penulisan ini diharapkan dapat memberikan pemahaman terkait bentuk-bentuk dan penerapan perlindungan hukum bagi korban tindak pidana pencurian data pribadi

c. Peneliti kemudian

Hasil penelitian ini diharapkan dapat meningkatkan wawasan dan pengetahuan terkait perlindungan hukum bagi korban tindak pidana pencurian data pribadi sehingga kedepannya dapat dijadikan referensi untuk penelitian selanjutnya.

E. Kerangka Teori dan Konseptual

1. Kerangka Teori

a. Masalah Pokok Kajian Hukum Pidana

Masalah pokok yang menjadi objek kajian hukum pidana menurut Tongat, 2009, meliputi Tindak Pidana, Pertanggungjawaban Pidana, Pidana, dan Masalah Korban[7].

Tindak pidana diterjemahkan dari bahasa Belanda "*Strafbaarfeit*" atau "*Delict*". Beberapa ahli terdapat perbedaan mengenai penerjemahan istilah "*Strafbaarfeit*", misalnya Moeljatno

[7] Tongat, *Dasar-dasar Hukum Pidana Indonesia Dalam Perspektif Pembaharuan*, UMM Press, Malang, 2009, Hal. 3.

menerjemahkan sebagai “Perbuatan Pidana”. Pengerian perbuatan pidana menurutnya adalah: “Perbuatan yang dilarang dan diancam pidana barangsiapa melanggar pelanggaran tersebut[8]”. Naskah Akademik RKUHP menggunakan istilah “Tindak Pidana” yang diartikan sebagai “Perbuatan melakukan atau tidak melakukan sesuatu yang oleh peraturan perundang-undangan dinyatakan sebagai perbuatan yang dilarang dan diancam dengan pidana”[9]. Secara garis besar persamaan definisi Tindak Pidana yaitu Perbuatan yang dilarang dan adanya ancaman pidana atas perbuatan tersebut.

Pertanggungjawaban pidana diterjemahkan dari *teorekenbaardheid* atau *criminal responsibility* yang artinya pemidanaan petindak dengan maksud untuk menentukan apakah seseorang terdakwa atau tersangka dapat dimintai pertanggungjawaban atas suatu tindakan pidana. Pertanggungjawaban pidana menurut Rancangan KUHP dibedakan menjadi 2 (dua) subjek, yaitu Pertanggungjawaban Pidana Orang dan Pertanggungjawaban Korporasi.

Pidana sering dikaitkan dengan Pemidanaan. Pidana adalah suatu penderitaan yang ditimpakan kepada seseorang . sedangkan pemidanaan menurut Andi Hamzah adalah suatu pengertian umum, sebagai suatu sanksi yang menderitakan atau nestapa yang sengaja

[8] Moeljatno, *Azas-azas Hukum Pidana*, Rineke Cipta, Jakarta, 1993, Hal. 56.
[9] Naskah Akademik RUU KUHP, Hal 179.

ditimpakan kepada seseorang. Pengertian yang diberikan oleh Andi Hamzah memberikan pengertian yang berbeda antara pemidanaan dan pidana, pemidanaan berbicara tentang sanksi yang menderitakan sedangkan pidana berbicara tentang hukum pidana itu sendiri.

Menurut kamus *Crime Dictionary*, Korban merupakan terjemahan dari Victim yang artinya adalah orang yang telah mendapat penderitaan fisik atau penderitaan mental, kerugian harta benda atau mengakibatkan mati atas perbuatan atau usaha pelanggaran ringan dilakukan oleh pelaku tindak pidana dan lainnya [10]. Kemudian secara Yuridis pengertian Korban juga termaktub dalam Undang-Undang Nomor 13 Tahun 2006 tentang Perlindungan Saksi dan Korban, yang menyatakan bahwa Korban adalah seseorang yang mengalami penderitaan fisik, mental, dan/atau kerugian ekonomi yang diakibatkan oleh suatu tindak pidana [11]. Lebih luas dijabarkan mengenai lingkup korban tidak hanya perseorangan, tetapi juga Institusi, Lingkungan Hidup, Masyarakat, dan Negara.

b. Teori Perlindungan Korban

Istilah perlindungan korban menurut Undang-Undang Nomor 13 Tahun 2006 tentang Perlindungan Saksi dan Korban selalu disertakan dengan Perlindungan Saksi. Di dalam undang-undang

[10] Bambang Waluyo, 2011, *Viktimologi Perlindungan Korban dan Saksi*, Jakarta: Sinar Grafika.
[11] Pasal 1 Angka (2) Undang-Undang Nomor 13 Tahun 2006 tentang Perlindungan Saksi dan Korban.

tersebut menggabungkan keduanya menjadi Perlindungan Saksi dan Korban. Istilah Korban telah diartikan sebagai seseorang atau objek lainnya yang telah mengalami penderitaan baik fisik, mental, maupun materiil karena akibat dari tindak pidana. Sedangkan istilah Perlindungan diartikan sebagai segala upaya pemenuhan hak dan pemberian bantuan untuk memberikan rasa aman kepada Saksi dan/atau Korban yang wajib dilaksanakan oleh Lembaga Perlindungan Saksi dan Korban (LPSK) atau lembaga lainnya sesuai dengan ketentuan Undang-Undang ini[12]. Perlindungan Saksi dan Korban bertujuan memberikan rasa aman kepada Saksi dan/atau Korban dalam memberikan keterangan pada setiap proses peradilan pidana.

Perlindungan Korban saat ini mengalami perluasan makna, pasalnya tindak pidana selain terjadi secara konvensional juga terjadi melalui dunia maya (*cyber crime*). Saat ini regulasi yang dipergunakan sebagai dasar hukum atas kasus-kasus *cybercrime* adalah Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE). Dengan adanya UU ITE ini diharapkan dapat melindungi masyarakat pengguna teknologi informasi di Indonesia, hal ini penting mengingat jumlah pengguna teknologi internet yang semakin meningkat dari tahun ke tahun.

[12] Pasal 1 Angka (6) Undang-Undang Nomor 13 Tahun 2006 tentang Perlindungan Saksi dan Korban.

Di dalam ketentuan Pasal 4 ayat (2) UU ITE disebutkan bahwa Pemerintah melindungi kepentingan umum dari segala jenis gangguan sebagai akibat penyalahgunaan Informasi Elektronik dan Transaksi Elektronik yang mengganggu ketertiban umum. Penyalahgunaan teknologi informasi pada umumnya dilakukan para *Hacker* atau *Cracker* yang tujuannya untuk mencuri data penting sehingga dapat merugikan seseorang, institusi, masyarakat, bangsa dan negara. *Hacker* atau *Cracker* beraksi dari tempat tertentu tanpa diketahui oleh pihak korban, aksinya tersebut dapat menimbulkan kerugian moril, materil maupun waktu akibat dari perusakan data korban.

c. Teori Penegakan Hukum

Penegakan hukum merupakan inti untuk mewujudkan keadilan dalam kehidupan bermasyarakat dan bernegara. Menurut ahli[13], Penegakan hukum merupakan rangkaian proses penjabaran ide dan cita hukum yang memuat nilai-nilai moral seperti keadilan dan kebenaran kedalam bentuk-bentuk konkrit, dalam mewujudkannya membutuhkan suatu organisasi seperti kepolisian, kejaksaan, pengadilan dan lembaga pemasyarakatan sebagai unsur klasik penegakan hukum yang dibentuk oleh negara, dengan kata lain

[13] Satjipto Rahardjo, 2009, *Penegakan Hukum : Suatu Tinjauan Sosiologis*, Yogyakarta: Genta Publishing, hal 5.

bahwa penegakan hukum pada hakikatnya mengandung supremasi nilai substansial yaitu keadilan.

Soerjono Soekanto[14], menjelaskan bahwa faktor-faktor yang mempengaruhi penegakan hukum meliputi: 1). Faktor hukumnya sendiri, yakni undang-undang; 2). Faktor penegak hukum, yakni pihak-pihak yang membentuk maupun menerapkan hukum; 3). Faktor sarana atau fasilitas yang mendukung penegakan hukum; 4). Faktor masyarakat, yakni lingkungan di mana hukum tersebut berlaku atau diterapkan; 5). Faktor kebudayaan, yakni sebagai hasil karya, cipta, dan rasa yang didasarkan pada karsa manusia di dalam pergaulan hidup. Dalam hal penegakan hukum terkait tindak pidana pencurian data pribadi, saat ini menggunakan payung hukum UU ITE.

2. Kerangka Konseptual

a. Perlindungan Hukum

Perlindungan hukum jika dipisahkan terdiri dari dua (2) kata yaitu Perlindungan dan Hukum yang masing-masing memiliki makna terpisah. Kata perlindungan mengandung makna suatu tindakan perlindungan atau tindakan melindungi dari pihak-pihak tertentu yang ditujukan untuk pihak tertentu dengan menggunakan cara-cara tertentu [15].

[14] Soerjono Soekanto, 2011, *Faktor-Faktor yang Mempengaruhi Penegakan Hukum*, Jakarta: PT. Raja Grafindo Persada, hal 8.

[15] Wahyu Sasongko, 2007, *Ketentuan-Ketentuan Pokok Hukum Perlindungan Konsumen*, Bandar Lampung: Universitas Lampung, Hal. 30.

Hukum menurut J.C.T Simorangkir[16], adalah peraturan-peraturan yang bersifat memaksa, yang menentukan tingkah laku manusia dalam lingkungan masyarakat yang dibuat oleh badan-badan resmi yang berwajib, pelanggaran mana terhadap peraturan-peraturan tadi berakibat diambilnya tindakan, yaitu dengan hukuman tertentu.

Kemudian jika digabungkan, Perlindungan Hukum adalah adanya upaya melindungi kepentingan seseorang dengan cara mengalokasikan suatu Hak Asasi Manusia kekuasaan kepadanya untuk bertindak dalam rangka kepentingannya tersebut[17]. Perlindungan hukum pada prinsipnya melindungi subyek hukum dalam bentuk perangkat hukum.

Meskipun dunia *Cyber* adalah virtual, perlindungan hukum tetap diperlukan untuk melindungi aktivitas subjek hukum dari *cybercrime*. Setidaknya ada dua alasan yaitu[18] : *Pertama* masyarakat yang ada didunia maya adalah masyarakat yang ada di dunia nyata, masyarakat memiliki nilai dan kepentingan baik secara sendiri-sendiri maupun bersama-sama harus dilindungi. *Kedua*, walaupun terjadi di dunia maya, transaksi yang dilakukan

[16] C.S.T. Kansil, 1989, *Pengantar Ilmu Hukum dan Tata Hukum Indonesia*, Jakarta: Balai Pustaka, Hal. 38.

[17] Satjito Rahardjo, 2003, *Sisi-Sisi Lain dari Hukum di Indonesia*, Jakarta: Kompas, Hal. 121.

[18] Josua Sitompul, 2012, *Cyberspace, cybercrime, Cyberlaw, Tinjauan Aspek Hukum Pidana*, Jakarta: PT. Tatanusa, Hal. 38.

oleh masyarakat memiliki pengaruh dalam dunia nyata, baik secara ekonomis maupun non ekonomis.

Saat ini perangkat hukum yang digunakan untuk melindungi subjek hukum dari *cybercrime* adalah Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) sebagaimana diubah dengan Undang-Undang Nomor 19 Tahun 2016. UU ITE spesifik mengatur mengenai ketentuan hukum siber atau dunia maya, didalamnya mengatur kewajiban-kewajiban pemilik sistem elektronik untuk memastikan keamanan dan kenyamanan pada sistem elektroniknya. Selain itu juga mengatur perlindungan hukum bagi korban atas kejahatan di dunia maya. Dalam perlindungan hukum terhadap korban *cybercrime* secara mendasar ada dua model yaitu model hak-hak prosedural dan model pelayanan.

Pada model hak prosedural, korban *cybercrime* diberikan hak untuk melakukan tuntutan pidana atau membantu penegak hukum, atau hak untuk dihadirkan pada setiap tingkatan peradilan diamana keterangannya dibutuhkan.

Sedangkan model pelayanan, lebih bertitik berat pada perlunya diciptakan standar-standar baku bagi pembinaan korban *cybercrime*. Model ini melihat korban sebagai sosok yang harus dilayani oleh aparat penegak hukum, dengan demikian korban

penyalahgunaan teknologi informasi ini akan lebih percaya institusi penegak hukum untuk mengatasi kasus *cybercrime*[19].

b. Korban *Cybercrime*

Korban *Cybercrime* yang diatur secara spesifik di dalam UU ITE yaitu setiap orang, badan usaha, atau negara yang dirugikan akibat penyalahgunaan teknologi informasi. Perbuatan penyalahgunaan teknologi informasi yang dapat merugikan korban diatur di dalam Pasal 26 hingga Pasal 37 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) sebagaimana diubah dengan Undang-Undang Nomor 19 Tahun 2016.

c. Pencurian Data Pribadi

Definisi data pribadi dapat ditemukan dalam peraturan perundang-undangan antara lain:

1) Pasal 1 Nomor 1 Peraturan Menteri Komunikasi dan Informatika No. 20 tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik menyebutkan bahwa data pribadi dimaksudkan sebagai identitas seseorang yang terang dan jelas yang merupakan penetapan bukti diri terhadapnya yang dipelihara, dijaga

[19] Muladi dan Barda Nawawi Arif, 1992, *Bunga Rampai Hukum Pidana*, Bandung: Alumni, Hal. 79.

kebenarannya dan ditempatkan dengan aman kerahasiannya.

2) Pasal 1 angka 29 Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, mendefinisikan Data Pribadi adalah setiap data tentang seseorang baik yang teridentifikasi dan/atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui Sistem Elektronik dan/atau nonelektronik.

3) Rancangan Undang-Undangan tentang Perlindungan Data Pribadi, mengklasifikasikan data pribadi terdiri atas data pribadi yang bersifat umum dan sensitif. Data pribadi yang bersifat umum meliputi: Nama, Tempat Tanggal Lahir, Nomor Kartu Tanda Pengenal (KTP, SIM, NPWP, Paspor, dsg), Data Biometrik. Data pribadi yang bersifat sensitif meliputi: Agama/ Keyakinan, Kesehatan, Kondisi Fisik/ Mental, Kebiasaan Pribadi, Kehidupan Seksual, Pandangan Politik, Catatan Kejahatan, Data Anak, Data Keuangan.

Menurut ketentuan Pasal 26 UU ITE, pengaturan mengenai penggunaan informasi yang ada di media elektronik berupa data pribadi seseorang harus dilakukan atas persetujuan pemiliknya.

Artinya apabila diakses dan dimanfaatkannya data pribadi tanpa persetujuan pemilik dapat disebut sebagai pencurian/ penyalahgunaan data pribadi. Pelanggaran atas ketentuan tersebut, korban dapat mengajukan gugatan ke pengadilan atas kerugian yang ditimbulkan.

Pencurian data pribadi dapat diartikan sebagai aktivitas mengambil data pribadi pengguna sistem elektronik dengan cara peretasan atau mengakses kedalam sistem elektronik secara ilegal. Sedangkan penyalahgunaan data pribadi dapat diartikan sebagai aktivitas yang menggunakan data pribadi seseorang untuk kepentingannya sendiri tanpa seizin dari pemilik data pribadi.

d. Sistem Elektronik

Sistem elektronik menurut UU ITE adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan Informasi Elektronik. Pihak yang menyediakan, mengelola, dan/atau mengoperasikan Sistem Elektronik disebut dengan Penyelenggara Sistem Elektronik (PSE).

PSE dikelompokkan menjadi dua (2) kategori[20], yaitu PSE Lingkup Publik dan PSE Lingkup Privat. PSE lingkup Publik terdiri dari Instansi dan Institusi yang ditunjuk Instansi kecuali otoritas pengatur dan pengawas sektor keuangan, misalnya Setneg dengan aplikasinya LAPOR, Peduli Lindungi Kemenkes, dan lain sebagainya. Sedangkan PSE lingkup Private yaitu PSE yang diawasi oleh Kementerian atau Lembaga berdasarkan ketentuan peraturan perundang-undangan, misalnya Gojek, Tokopedia, OLX, Shopee dan lain sebagainya.

F. Metode Penelitian

1. Sifat Penelitian

   Penelitian ini merupakan penelitian hukum yang bersifat **Deskriptif Analitis**, yaitu memaparkan data-data mengenai bentuk-bentuk dan upaya perlindungan hukum terhadap korban pencurian data pribadi. Sifat penelitian ini dipilih karena merupakan sifat penelitian yang cukup baik untuk memaparkan karakteristik suatu fenomena.

2. Metode Pendekatan

   Metode Pendekatan yang digunakan di dalam penelitian ini yaitu **Pendekatan Yuridis Normatif** khususnya pendekataan perundang-undangan dan pendekatan konsep. Pendekataan perundang-undangan dilakukan dengan cara inventarisasi hukum positif berupa peraturan perundang-undangan dan rancangan peraturan perundang-undangan

[20] Pasal 2 ayat (2) Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik

serta instrumen hukum lainnya yang ada kaitannya dengan pencurian data pribadi antara lain UU ITE, PP PSTE, Peraturan Kominfo dan lain lain. Sedangkan untuk pendekatan konsep bersumber pada RUU Perlindungan Data Pribadi. Kemudian dikaitkan dengan pendapat-pendapat dan hasil penelitian para sarjana serta data berupa bahan dari kamus hukum.

3. Metode Pengumpulan Data

   Metode Pengumpulan Data menggunakan teknik Studi Pustaka dan Studi Dokumen. Data atau bahan hukum yang digunakan di dalam skripsi ini dibedakan menjadi 3 kategori yaitu: (1) Bahan Hukum Primer berupa UU ITE, PP PSTE, KUHP, KUHAP, dan hasil wawancara di lingkungan Direktorat Operasi Keamanan Siber, BSSN. (2) Bahan Hukum Sekunder yang digunakan berupa buku-buku terkait hukum pidana, buku terkait hukum siber, RUU Perlindungan Data Pribadi, artikel atau makalah terkait pelindungan data pribadi. (3) Bahan Hukum Tersier yang digunakan berupa kamus hukum dan ensiklopedia hukum.

4. Metode Analisis Data

   Metode analisis data menggunakan metode **Analisis Kualitatif** yaitu dengan cara melakukan analisis secara naratif dengan cara mempertemukan antara data-data hasil penelitian dengan teori-teori dan konsep kemudian diolah dan dianalisis dengan metode deduktif.

G. Sistematika Penulisan

Sistematika penulisan yang akan disajikan di dalam penulisan skripsi ini yaitu:

1. Bab I Pendahuluan

   Bab I Pendahuluan menjelaskan tentang Latar Belakang Masalah, Rumusan Masalah, Tujuan dan Manfaat Penulisan, Kerangka Teori dan Konseptual, Metode Penelitian, dan Sistematika Penulisan.

2. Bab II Tinjauan Pustaka tentang Kejahatan Siber, Pencurian Data Pribadi, Korban, dan Perlindungan Hukum.

3. Bab III Fakta/ Objek Penelitian

   Fakta/ Objek Penelitian di dalam skripsi ini menjelaskan mengenai korban pencurian data pribadi, target pencurian data pribadi, dan modus pelaku pencurian data pribadi.

4. Bab IV Analisis Yuridis Perlindungan Korban Tindak Pidana Pencurian Data Pribadi Melalui Sistem Elektronik

   Pada Bab IV Analisis Yuridis membahas mengenai modus terjadinya pencurian data pribadi melalui sistem elektronik, bentuk bentuk perlindungan hukum korban tindak pidana pencurian data pribadi

dalam hukum positif Indonesia, dan implementasi atau penerapan perlindungan terhadap korban tindak pidana pencurian data pribadi.

5. Bab V Penutup

   Pada Bab V Penutup mengemukakan mengenai kesimpulan yang dihasilkan selama poses penulisan dan saran yang dapat diberikan penulis kepada pembaca maupun pihak terkait dari hasil penulisan.

Daftar Pustaka

Lampiran