BAB I
PENDAHULUAN

A. Latar Belakang

IPTEK (Ilmu Pengetahuan dan Teknologi), yang dari masa ke masa semakin maju dan berkembang. Saat ini ilmu pengetahuan dan teknologi berkembang amat cepat terutama di bidang komputer, yang sekarang ini sudah menjadi realita sehari-hari bahkan merupakan tuntutan masyarakat yang tidak dapat ditawar lagi. Dari itulah timbul apa yang disebut dengan bidang informasi, yang merupakan titik sentral dalam banyak kehidupan manusia tidak terkecuali bidang hukum. Saat ini kebutuhan manusia akan teknologi informasi tersedia dengan bebas dan tanpa batas. Namun dari keadaan tersebut disamping banyak manfaat yang diberikan kepada pemenuhan kebutuhan manusia akan informasi dalam melakukan aktivitas hidupnya juga memberikan pengaruh yang tidak baik.

Teknologi yang sebenarnya merupakan alat bentu/ekstensi kemampuan diri manusia, dewasa ini telah menjadi sebuah kekuatan otonom yang justrumembelenggu perilaku dan gaya hidup kita sendiri. Dengan daya pengaruhnya yang sangat besar, karena ditopang pula oleh sistem-sistem sosial yang kuat, dan dalam kecepatan yang makin tinggi, teknologi telah menjadi pengarah hidup manusia. Masyarakat yang rendah kemampuan teknologinya cenderung tergantung dan hanya mampu bereaksi terhadap dampak yang ditimbulkan oleh kecanggihan teknologi.

Teknologi yang sebenarnya merupakan alat bentu/ekstensi kemampuan diri manusia, dewasa ini telah menjadi sebuah kekuatan otonom yang justru membelenggu perilaku dan gaya hidup kita sendiri. Dengan daya pengaruhnya yang sangat besar, karena ditopang pula oleh sistem-sistem sosial yang kuat, dan dalam kecepatan yang makin tinggi, teknologi telah menjadi pengarah hidup manusia. Masyarakat yang rendah kemampuan teknologinya cenderung tergantung dan

hanya mampu bereaksi terhadap dampak yang ditimbulkan oleh kecanggihan teknologi.[2]

Pada satu sisi, perkembangan dunia IPTEK yang demikian mengagumkan itu memang telah membawa manfaat yang luar biasa bagi kemajuan peradaban umat manusia. Jenis-jenis pekerjaan yang sebelumnya menuntut kemampuan fisik yang cukup besar, kini relatif sudah bisa digantikan oleh perangkat mesin-mesin otomatis, Demikian juga ditemukannya formulasi-formulasi baru kapasitas komputer, seolah sudah mampu menggeser posisi kemampuan otak manusia dalam berbagai bidang ilmu dan aktifitas manusia. Kemajuan teknologi informas yang serba digital membawa orang ke dunia bisnis yang revolusioner (digital revolution era) karena dirasakan lebih mudah, murah, praktis dan dinamis berkomunikasi dan memperoleh informasi.[3]

Di sisi lain, berkembangnya teknologi informasi menimbulkan pula sisi rawan yang gelap sampai tahap mencemaskan dengan kekhawatiran pada perkembangan tindak pidana di bidang teknologi informasi yang berhubungan dengan kejahatan mayantara atau ‘‘cybercrime’’. Masalah kejahatan mayantara dewasa ini sepatutnya mendapat perhatian semua pihak secara seksama pada perkembangan teknologi informasi masa depan, karena kejahatan ini termasuk salah satu extra ordinary crime (kejahatan luar biasa) bahkan dirasakan pula sebagai serious crime (kejahatan serius) dan transnational crime (kejahatan antar negara) yang selalu mengancam kehidupan warga masyarakat, bangsa dan negara.

Tindak pidana atau kejahatan ini adalah sisi paling buruk di dalam kehidupan moderen dari masyarakat informasi akibat kemajuan pesat teknologi dengan meningkatnya peristiwa kejahatan komputer, pornografi, terorisme digital, “perang” informasi sampah, bias informasi, hacker, cracker, dan sebagainya. Oleh karena itu tidaklah salah apabila perkembangan teknologi informasi harus diperhatikan dan diawasi dengan sebaik-baiknya, untuk mencegah timbulnya

[2] Abdul Wahid dan Mohammad Labib, *Kejahatan Mayantara (cybercrime*), (Refika Aditama: Bandung, 2005). hal.140-150

[3] Cahyo Handoko, Kedudukan Alat Bukti Digital Dalam Pembuktian CyberCrime di Pengadilan, *Jurisprudentie*, Vol. 6 No. 2. 2019. hal 40

berbagai macam kejahatan yang memanfaatkan dan yang diakibatkan oleh perkembangan teknologi.[4]

Kejahatan *cyber* adalah suatu tindakan kejahatan yang berkaitan dengan komputer maupun perangkat jaringan, biasanya kejahatan ini dilakukan secara online. bahkan kejahatan cyber ini bisa menargetkan siapa saja, Jika kalian menjadi salah satu korbannya, tentu akan mengakibatkan banyak merugikan. Bahkan berpengaruh pada kondisi mental hingga kerugian secara finansial. Salah satu contoh dari *cyber crime* yang sangat berbahaya adalah *Doxxing*, yang berujung pada *cyberbullying* hingga pengambilan data pribadi dan menyebarkannya di internet. Tujuan dari tindakan ini sangat bermacam-macam. Mulai dari ancaman, pemerasan, mempermalukan seseorang dan mengambil keuntungan yang lainnya.

Kejahatan mayantara (*cybercrime*) adalah salah satu bentuk atau dimensi baru dari kejahatan masa kini yang diakibatkan oleh perkembangan teknologi yang sangat pesat. Kejahatan ini bahkan sudah menjadi perhatian dunia internasional. Kejahatan mayantara atau cybercrime merupakan salah satu sisi gelap dari kemajuan teknologi yang mempunyai dampak negatif sangat luas bagi seluruh bidang kehidupan modern saat ini. Cybercrime adalah perbuatan melawan hukum yang dilakukan dengan menggunakan internet yang berbasis pada kecanggihan teknologi komputer dan telekomunikasi. Cybercrime sebenarnya bukan hanya menggunakan kecanggihan teknologi komputer akan tetapi juga memanfaatkan teknologi informasi dalam pengoperasiannya.

Hacking Sim Card atau *Sim Card Swapping*, adalah kegiatan pembobolan data di mana hacker akan menelepon layanan penyedia sim card dan mengaku sebagai pemilik nomor. Yang dimana biasanya di dalam sim card terebut terdapat data pribadi seseorang yang dimana terdapat nomor induk kependudukan atau yang biasa disebut NIK dan Nomer Kartu Kelurga, yang merupakan data pribadi yang sangat penting bagi seseorang. Muncul kembalinya aktivitas *cyberattack* ini

[4] Abdul Wahid dan Mohammad Labib. Kejahatan Mayantara (cybercrime), (Refika Aditama: Bandung, 2005), hal 80-85

disebabkan oleh kecerobohan yang kerap dilakukan banyak orang. Kecerobohan yang dimaksud adalah menyebarkan data-data pribadi di internet dengan mudah. Namun, dalam beberapa kasus, data para korban juga bisa bocor saat mereka bercakap dengan operator layanan sim card terkait proses identifikasi. Pasalnya awal mula perencanaan hacking sim card adalah untuk mengetahui identitas serta data singkat dari korban. Hal ini dibutuhkan hacker ketika ia akan meminta layanan penyedia sim card untuk kartu baru. Bila hacker sudah memiliki data-data terkait permintaan kartu sim baru, maka mereka bisa dengan mudah memenangkan akses ke dokumen penting milik korban.

Kartu SIM dapat dimanipulasi melalui SIM swap, yaitu modus penipuan dengan mengambil alih nomor ponsel atau kartu SIM dengan cara menduplikasinya melalui operator seluler.Dalam kejahatan ini korban biasanya tak mengerti apa yang terjadi, dan tak tahu apa yang harus dilakukan. Dengan menduplikasi kartu SIM, pelaku dapat menggandakan identitas, mengambil alih akun media sosial dan mengambil alih akun bank.Dengan tiga tindakan tersebut berbagai macam kejahatan siber dapat dilakukan dan bukan hanya mengancam pemilik nomor ponsel tetapi juga semua orang yang terafiliasi dengan nomor ponsel tersebut dan akun-akun yang dikuasai.Perentasan Kartu SIM sebenarnya dilakukan dengan cara yang sangat sederhana[5] Cara ini bahkan dapat dilakukan oleh siapa saja tanpa ada yang akan menaruh curiga, berikut trik yang biasa dilakukan:

a) Pelaku memperoleh data pribadi korban melalui pembobolan data, phising, pencarian media sosial, aplikasi jahat, belanja online, malware, dan lain-lain.
b) Dengan informasi ini, pelaku menipu operator ponsel untuk menduplikasi nomor ponsel korban ke SIM miliknya.
c) Operator seluler menonaktifkan kartu SIM asli dan mengeluarkan yang baru untuk pelaku.

[5] Kusnadi, S. A, Perlindungan Hukum Data Pribadi Sebagai Hak Privasi, *AL WASATH Jurnal Ilmu Hukum*, 2021, hal. 15

d) Pelaku sekarang dapat menerima panggilan masuk dan pesan teks, termasuk akses ke perbankan online korban.
e) Korban akan melihat ponsel kehilangan layanan, dan akhirnya akan mengetahui bahwa mereka tidak dapat masuk ke akun-akun mereka termasuk akun perbankannya.

Proses peretasan kartu SIM akan sangat mudah dilakukan di Indonesia, hal ini tidak lepas dari lemahnya sistem validasi di Indonesia. Operator seluler sejauh ini hanya melakukan pemeriksaan secara manual, tidak ada sistem verifikasi yang terintegrasi untuk memastikan bahwa data yang mereka terima benar asli atau tidak. Baru ini fenomena kebocoran data yang meresahkan masyarakat Indonesia, Teguh Aprianto, Konsultan Keamanan Siber dan Pendiri Ethical Hacker Indonesia, mengatakan bahwa ada dugaan bahwa sebanyak 1,3 Miliar SIM Card Seluler Indonesia telah bocor dari Kementerian Komunikasi dan Informatika berdasarkan data aktivasi SIM Card. 1,3 miliar data kartu registrasi sim prabayar yang bocor. Kebocoran data berjumlah 1.304.401.300 diunggah oleh akun bernama Bjorka dalam forum Breached.to. Data sebesar 87 GB diklaim berisi NIK, nomor ponsel, provider telekomunikasi, dan tanggal registrasi [6]. Indonesia sebagai Negara kebocoran data terbesar di Asia sampai sekarang. Ia mengingatkan bahwa dalam soal registrasi ini ada tiga pihak yang harus bertanggung jawab, pertama adalah Kominfo itu sendiri sebagai pihak yang mewajibkan, kedua adalah operator dalam hal ini penyelenggara jasa telekomunikasi, lalu yang ketiga adalah Dukcapil. Permasalahan lain yang akan timbul yaitu data diri pengguna disebar di berbagai media sosial *(doxing). Doxing* atau *dropping documents* adalah tindakan berbasis internet untuk meneliti dan menyebarkan informasi pribadi (termasuk data pribadi) individu atau organisasi kepada public. *Doxing* jenis ini mengungkapakan identitas seseorang melalui keberadaan fisik seperti nomor telepon atau email yang kemudian mengadakan kejelasan yang meliputi tempat tinggal atau tempat seseorang bekerja.

[6] Lahur, M. F, Perentasan Hak Pribadi. *Jurnal Hukum*, 2021, hal, 3-10

Meningkatnya kasus kejahatan kebocoran data pribadi akibat peretasan yang memanfaatkan teknologi informasi yang teridentifikasi pada tahun 2022, dengan contoh kasus kebocoran data pengguna aplikasi e-HAC KeMenKes, kebocoran data NIK pengguna nomor telpon, kebocoran data BPJS Kesehatan, kebocoran data nasabah BRI Life, kebocoran data DPT pemilu KPU, kebocoran data pengguna Tokopedia, sertfikat vaksin Presiden RI, data pribadi situs media sosial seperti Instagram dan Facebook, data indiHome dan masih banyak yang lainnya. Selain itu, pengelolaan informasi data khususnya pengelolaan data pribadi, merupakan salah satu peluang kejahatan dalam perkembangan teknologi informasi. Karena berbagai data informasi pribadi tidak sukar untuk diakses sehingga diperlukannya perlindungan data pribadi. Batasan privasi semakin tipis akibat kemajuan teknologi informasi dan komunikasi.[7]

Dengan mengirimkan Nomor Induk Kependudukan (NIK) dan Nomor Kartu Keluarga (KK) melalui pesan singkat, pengguna kartu prabayar seluler harus mendaftarkan informasi pribadinya, yang kemudian disinkronkan dengan data dari Ditjen Kemendagri Kependudukan Catatan Sipil.Secara teknis, pemerintah mengumpulkan data registrasi kartu SIM, namun pesan pelanggan terlebih dahulu masuk ke SMS milik provider. Proses penguncian data ini berisiko karena tidak ada cara untuk memastikan bahwa informasi pribadi pelanggan dilindungi dan dirahasiakan.[8]

Kemajuan teknologi telah merubah struktur masyarakat dari yang bersifat lokal menuju ke arah masyarakat yang berstruktur global. Perubahan ini disebabkan oleh kehadiran teknologi informasi. Perkembangan teknologi informasi itu berpadu dengan media dan komputer, yang kemudian melahirkan piranti baru yang disebut internet. Kehadiran internet telah memunculkan paradigma baru dalam kehidupan manusia. Kehidupan berubah dari yang hanya

---

[7] Kusnadi, S. A, Perlindungan Hukum Data Pribadi Sebagai Hak Privasi, *AL WASATH Jurnal Ilmu Hukum*, 2021, Hal, 9-10

[8] Apryan Angga, Hacker Bjorka Berperan Dalam Kebocoran Data Pribadi, *Jurnal Hukum Magnum Opus*, Volume 6 Nomor 1,2023, hal. 2-7

bersifat nyata (real) ke realitas baru yang bersifat maya (virtual). Realitas yang kedua ini biasa dikaitkan dengan internet dan *cyberspace*.

Perkembangan Internet yang semakin hari semakin meningkat, baik perangkat maupun penggunaannya, membawa dampak positif atau pun negatif. Teknologi selain membawa keuntungan berupa semakin dipermudahnya hidup manusia, juga membawa kerugian-kerugian berupa semakin dipermudahnya penjahat untuk melakukan kejahatan. Teknologi juga memberikan pengaruh yang signifikan dalam pemahaman mengenai kejahatan terutama terhadap aliran-aliran dalam kriminologi yang menitik beratkan pada faktor manusia, baik secara lahir maupun psikologis. Kejahatan sebenarnya telah ada sejak awal zaman, hingga sekarang. Seiring dengan perkembangan zaman bentuk-bentuk kejahatanpun semakin bervariasi. Perkembangan teknologi merupakan salah satu faktor yang dapat menimbulkan kejahatan. Seiring dengan perkembangan teknologi, maka jenis jenis kejahatan semakin berkembang dan bervariasi. Banyak kejahatan-kejahatan baru yang bermunculan dengan semakin berkembangnya teknologi, khususnya teknologi internet.[9]

Istilah "perlindungan data" umumnya mengacu pada prosedur yang mengikat, pengamanan, dan aturan yang berlaku untuk tetap mengontrol subjek data dan melindungi data pribadi. Intinya, pemilik data harus dapat memilih apakah akan membagikan data tertentu ataupun tidak, serta siapa saja yang dapat mengaksesnya, untuk seberapa lama, dan untuk tujuan apa. Pada pasal 58 ayat 1 Undang Undang Nomor 27 Tahun 2022 di sebutkan bahwa pemerintah berperan dalam mewujudkan penyelenggaraan perlindungan data pribadi dan pada pasal 47 Undang Undang nomor 27 tahun 2022 juga di sebutkan bahwa Pengedali Data Pribadi dalam hal ini pemerintah wajib bertanggung jawab atas pemrosesan Data Pribadi dan menunjukkan pertanggungjawaban dalam pemenuhan kewajiban pelaksanaan prinsip Perlindungan Data Pribadi. [10]

---

[9] Shinta Rajni, Skripsi Perlindungan Hukum Terhadap Data Pribadi Pengguna Jasa Telekomunikasi Atas Registrasi Kartu Prabayar, (Jakarta: UIN Syarif Hidayatullah, 2020), hal. 5

[10] Undang Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi

Pasal 1365 KUHPerdata pada dasarnya menjelaskan bahwa segala tindakan hukum yang merugikan orang lain, kemudian individu menimbulkan kerugian itu harus diberi ganti rugi dan Pasal 12 ayat (1) UU PDP Subjek Data Pribadi berhak menggugat dan menerima ganti rugi atas pelanggaran pemrosesan Data Pribadi tentang dirinya sesuai dengan ketentuan perundang-undangan yang merupakan dasar hukum yang dapat dijadikan sebagai dasar pengajuan gugatan atas kebocoran data akibat peretasan atau kesalahan. Berdasarkan latar belakang tersebut, penulis hendak melakukan penelitian mengenai Kejahatan CyberCrime yang berkaitan dengan Hacking Sim Card. Penulis menuangkan dalam bentuk proposal skripsi yang berjudul *"Kejahatan Cybercrime Hacking Sim Card Tentang Data Pribadi Dalam Prespektif Hukum"*

B. Rumusan Masalah

Berdasarkan uraian masalah pada latar belakang,penulis mengambil rumusan masalah dalam proposal ini adalah sebagai berikut:

1. Bagaimana perlidungan data pribadi terhadap hacking sim card dalam Prespektif Hukum?
2. Bagaimana hacking sim card terhadap data pribadi?

C. Tujuan Penelitian

Pada penelitian ini tujuan yang diharapkan adalah sebagai berikut:

1. Untuk mengetahui perlindungan data pribadi terhadap data pribadi seseorang
2. Untuk mengetahui dampak hacking sim card.
3. Untuk mengetahui bagaimana proses hacking sim card untuk memperoleh data pribadi

D. Kegunaan Penelitian

Pada penelitian ini diharapkan dapat bermanfaat untut:

1. Manfaat Teoritis

Penelitian ini diharapkan dapat bermanfaat bagi masyarakat pada umumnya, dan bagi penulis pada khususnya, mengenai pentingnya memahami apa itu cybercrime yang dalam hal ini berbentuk sebuah kejahatan yang berupa hacking sim card.Dengan tujuan masyarakat dan penulis lebih berhati hati

2. Manfaat Praktis

a. Bagi Pemerintah

Manfaat penelitian ini adalah sebagai masukan bagi pemerintah dalam hal ini pengedali data pribadi masyarakat lebih bertanggung jawab menjaga data pribadi dari hacker sim card yang sangat meresahkan bagi masyarakat

b. Bagi Masyarakat

Hasil penelitian ini diharapkan dapat memberikan informasi dan pembelajaran mengenai perkembangkan teknologi yang menjadi sasaran kejahatan cybercrime khususnya hacking sim card agar masyarakat lebih berhati hati dan tetap waspada

c. Bagi Peneliti

Penelitian ini menjadi ruang belajar dalam peningkatan kapasitas dan pengalaman berkaitan perkembangan teknologi yang dalam hal ini menjadi ladang kejahatan cybercrime yang dilakukan para hacker yang dalam hal ini melakukan kejahatan hacking sim card. Disamping itu penelitian ini merupakan salah satu syarat yang wajib dipenuhi bagi setiap mahasiswa untuk meraih gelar sarjana.

E. Penegasan Istilah

Pada kerangka awal guna mendapatkan gambaran yang jelas dan memudahkan memahami skripsi ini, maka perlu adanya ulasan terhadap penegasan arti dan maksud dari beberapa istilah yang terkait dengan judul skripsi ini. Berdasarkan penegasan ini diharapkan tidak akan terjadi kesalah pahaman terhadap pemaknaan judul dari beberapa istilah yang digunakan pada skripsi ini. Skripsi ini Penegasan Oprasional dari judul *“Pengaruh Teknologi Digital Terhadap Kejahatan Cybercrime Hacking Sim Card dalam Prespektif Hukum”* ini

adalah sebagai bentuk wujud rasa waspada dalam melakukan validasi sim card atau memasukkan sim card dan tujuan serta ruang lingkup maka perlu adanya penengasan judul secara konseptual dan oprasional sebagai berikut.

1. Penegasan Konseptual

Untuk memudahkan dan menghindari kesalahpahaman dalam mengartikan serta penafsiran terhadap istilah ataupun kata-kata yang ada di dalam penelitian ini, maka perlu adanya penjelasan mengenai hal-hal yang akan menjadi hal-hal yang nantinya akan menjadi pegangan dalam penelitian. Adapun penelitian ini dapat dijelaskan sebagai berikut.

a. Kejahatan *Cybercrime*

Kejahatan komputer atau kejahatan cyber atau kejahatan dunia maya *(cybercrime)* adalah sebuah bentuk kriminal yang mana menjadikan internet dan komputer sebagai medium melakukan tindakan kriminal.Masalah yang berkaitan dengan kejahatan jenis ini misalnya hacking, pelanggaran hak cipta, pornografi anak, dan eksploitasi anak.Juga termasuk pelanggaran terhadap privasi ketika informasi rahasia hilang atau dicuri, dan lainnya.Dalam definisi lain, kejahatan dunia maya adalah istilah yang mengacu kepada aktivitas kejahatan dengan komputer atau jaringan komputer menjadi alat, sasaran atau tempat terjadinya kejahatan[11].

Cybercrime ini potensial meimbulkan kerugiann pada beberapa bidang: politik, ekonomi, sosial budaya yang signifikan dan lebih memperhatika dibandigkan degan kejahatan yag berintensitas tinggi lainnya *Cybercrime* adalah sebuah perbuatan yang tecela dan melanggar kepatutan di dalam kehidupan mayarakat serta melanggar hukum, sekalipun sampai sekarang sukar untuk menemukan norma hukum yang secara khusus mengatur *cybercrime*. Oleh karena itu peran masyarakat dalam upaya menegakan hukum terhadap *cybercrime* adalah penting untuk

[11] Ricky Adjie Purnama, "Cyber Crime Dalam Perspektif Hukum Positif dan Hukum Islam", (Skripsi), Fakultas Syari"ah IAIN SMH Bante, 2007, hal.12

menentukan sifat dapat dicela dan melanggar kepatutan masyarakat dari suatu perbuatan *cybercrime*.[12]

Berbicara masalah *cybercrime* tidak lepas dari permasalahan keamanan[13] jaringan komputer atau keamanan informasi berbasis internet dalam era global ini, apalagi jika dikaitkan dengan persoalan informasi sebagai komoditi. Informasi sebagai komoditi memerlukan kehandalan pelayanan agar apa yang disajikan tidak mengecewakan pelanggan. Untuk mencapai tingkat kehandalan tentang informasi itu sendiri harus selalu dimutaakhirkan sehingga informasi yang disajikan tidak ketinggalan zaman. Kejahatan dunia maya (*cybercrime*) ini muncul seiring dengan perkembangan teknologi informasi yang begitu cepat.

b. Hacking Sim Card

Hacking *Sim Card* atau *Sim Card Swapping*, adalah kegiatan pembobolan data di mana hacker akan menelepon layanan penyedia sim card dan mengaku sebagai pemilik nomor.Yang dimana biasanya di dalam sim card terebut terdapat data pribadi seseorang yang dimana terdapat nomor induk kependudukan atau yang biasa disebut NIK dan Nomer Kartu Kelurga,yang merupakan data pribadi yang sangat penting bagi seseorang. Muncul kembalinya aktivitas *cyberattack* ini disebabkan oleh kecerobohan yang kerap dilakukan banyak orang. Kecerobohan yang dimaksud adalah menyebarkan data-data pribadi di internet dengan mudah. Namun, dalam beberapa kasus, data para korban juga bisa bocor saat mereka bercakap dengan operator layanan sim card terkait proses identifikasi[14]

c. Data Pribadi

---

[12] Abdul Wahid dan Mohammad Labib, *Kejahatan Mayantra (Cyber Crime*), (Bandung: PT Refika Aditama, 2005), hal. 65

[13] Dikdik M. Arief Mansur, dan Elisatris Gultom, *Cyber Law Aspek Hukum Teknologi Informasi*, (Bandung Pt. Grafika Aditama 2005), hal. 89

[14] Radian Adi Nugraha, *Analisis Yuridis Mengenai Perlindungan Data Pribadi Dalam Cloud Computing System Ditinjau Dari Undang-undang Informasi Dan Transaksi Elektronik*, (Skripsi), (Fakultas Hukum Universitas Indonesia, 2012), hal. 19-20.

Data pribadi adalah data yang berkenaan dengan ciri seseorang, nama, umur, jenis kelamin, pendidikan, pekerjaan, alamat, dan kedudukan dalam keluarga.Pengertian lain dari "data pribadi" adalah data yang berupa identitas, kode, simbol, huruf atau angka penanda personal seseorang yang bersifat pribadi dan rahasia. Dalam Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik pada Pasal 1 angka 1 menjelaskan mengenai definisi data pribadi, yaitu data perseorangan tertentu yang disimpan, dirawat, dan dijaga kebenaran serta dilindungi kerahasiannya.[15]

d. Perlindungan Data Pribadi

Perlindungan Data Pribadi adalah segala upaya yang dilakukan untuk melindungi data pribadi individu dalam rangkaian pemrosesan atau pengelolaan data pribadi untuk menjamin hak konstitusional Subjek Data Pribadi.

Pada prinsipnya bentuk perlindungan terhadap data pribadi dibagi dalam dua bentuk, yaitu bentuk perlindungan data berupa pengamanan terhadap fisik data itu,baik data yang kasat mata maupun data yang tidak kasat mata. Bentuk perlindungan data yang kedua adalah adanya sisi regulasi yang mengatur tentang penggunaan data oleh orang lain yang tidak berhak, penyalahgunaan data untuk kepentingan tertentu, dan pengrusakan terhadap data itu sendiri

2. Penegasan Oprasiona

Penegasan Oprasional dari judul *"Analisis Pengaruh Teknologi Digital Terhadap Kejahatan Cybercrime Dalam Perspektif Undang Undang Perlindungan Data Pribadi Terkait Hacking Sim Card"* ini adalah bentuk pemahaman khusus dalam memahami atau menganalisa kejahatan cybercrime dalam bentuk hacking sim card yang berguna untuk mewujudkan masyarakat yang aman dan tenang dan menciptakan masyarakat yang peduli dengan data

[15] Rosalinda Elsina Latumahina, Aspek Hukum Perlindungan Data Pribadi di Dunia Maya, *Jurnal Gema Aktualita*, Vol. 3, No. 2, 2014, hlm 16.

pribadi nya dan lebih berhati hati dalam mengisi data pribadi nya terutama untuk pemerintah untuk selalu bertanggung jawab menjaga data pribadi masyrakat Indonesia dari serangan oknum yang tidak bertanggung jawab atau yang disebut hacker [16]

F. METODE PENELITIAN

1. Jenis Penelitian

Jenis penelitian ini adalah penelitian hukum normatif (normative law research) menggunakan studi kasus normatif berupa produk perilaku hukum. Penelitian hukum normatif atau biasanya dikenal dengan studi dokumen, menggunakan metode kualitatif untuk menganalisis data, dan menggunakan data sekunder yang digunakan sebagai sumbernya. Pokok kajiannya adalah hukum yang dikonsepkan sebagai norma atau kaidah yang belaku dalam masyarakat dan menjadi acuan perilaku setiap orang. Sehingga penelitian hukum normatif berfokus pada inventarisasi hukum positif, asasasas dan doktrin hukum, penemuan hukum dalam perkara in concreto, sistematik hukum, taraf sinkronisasi, perbandingan hukum dan sejarah hukum.

Pendekatan yang digunakan dalam penelitian ini adalah pendekatan perundangundangan (statue approach) yaitu dilakukan dengan menelaah semua undang-undang dan regulasi yang bersangkut paut dengan isu hukum yang sedang ditangani. Hasil dari telaah tersebut merupakan suatu argument untuk memecahkan isu yang dihadapi.Adapun pendekatan historis (historical approach) yang dilakukan dengan menalaah latar belakang apa yang dipelajari dan perkembangan pengaturan mengenai isu yang dihadapi. Telaah demikian diperlukan oleh peneliti manakala peneliti memang ingin mengungkap filosofis dan pola pikir yang melahirkan sesuatu yang sedang dipelajari. Adapun pendekatan kasus (case approach) adalah pendekatan yang dilakukan dengan cara melakukan telaah terhadap kasus-kasus yang berkaitan

[16] Ricky Adjie Purnama, "Cyber Crime Dalam Perspektif Hukum Positif dan Hukum Islam", (Skripsi. Fakultas Syari"ah IAIN SMH Bante, 2007), hal. 14

dengan isu yang dihadapi yang telah menjadi putusan pengadilan yang telah mempunyai kekuatan hukum yang tetap. Adapun yang terakhir pendekatan konseptual (conseptual approach) yaitu berasal dari pandangan-pandangan dan doktrin-doktrin yang berkembang di dalam ilmu hukum.[17]

2. Sumber Data

Sumber data yang digunakan dalam penelitian ini dapat dikelompokkan menjadi dua jenis, yaitu :

1) Bahan primer, yaitu yang digunakan penyusun dalam penulisan ini peraturan perundang-undangan yang mengatur tentang cybercrime dan hacking simcard:
   a) Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi
   b) Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen
   c) Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia
   d) Undang-Undang Nomor 24 Tahun 2013 tentang Admnistrasi Kependudukan
   e) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE)
   f) Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik
   g) Undang Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi
   h) Peraturan Menteri Komunikasi dan Informatika (Permenkominfo) Republik Indonesia Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik.

[17] Soerjono Soekanto, *Pengantar Penelitian Hukum*, (UI-Press: Jakarta, 1981), hlm. 43

2) Bahan Sekunder yaitu berupa buku-buku hukum termasuk skripsi, tesis, dan disertasi, dan jurnal-jurnal hukum. Kegunaan bahan hukum sekunder adalah memberikan kepada peneliti semacam "petunjuk" ke arah mana peneliti melangkah

3. Teknik Pengumpulan Data

Studi kepustakaan yaitu pengumpulan data melalui buku-buku tentang hukum, Undang-Undang, Peraturan Pemerintah dan sumber lain yang berkaitan dengan penelitian untuk mendapatkan landasan teoritis. Pengumpulan data hukum dilakukan dengan cara mencatat segala informasi terkini tentang isu dalam penelitian. Disamping itu juga penelitian dilakukan melalui meneliti buku-buku literature untuk mendapatkan landasan teoritis pendapat para ahli[18]

4. Teknik Penyajian Data

Hasil penelitian ini disajikan dalam bentuk uraian-uraian yang tersusun secara sistematis, yaitu data sekunder yang diperoleh akan dihubungkan satu dengan lainnya yang disesuaikan dengan permasalahan yang diteliti, sehingga secara keseluruhan merupakan kesatuan yang utuh sesuai dengan kebutuhan yang diteliti

5. Teknik Analisis Data

Teknik analisis data yang digunakan adalah analisis kualitatif, yakni dengan menganalisis data-data sekunder yang didapat sesuai dengan rumusan masalah yang telah ditentukan. Dengan metode kualitatif artinya dalam bentuk kalimat-kalimat yang disusun secara sistematis berdasarkan pada asas dan prinsip hukum yang berlaku. Dari analisis yang dilakukan kemudian menghasilkan kesimpulan dan rekomendasi.

[18] Koentjaranigrat, *Pengantar Penelitian Hukum*, (Gramedia: Sumatera Barat, 1987), hal 43-44