

BAB I

PENDAHULUAN

1.1 Latar Belakang

Saat ini perkembangan teknologi dan internet sudah sangat pesat, semua sudah dibuat menjadi lebih mudah. Salah satu sektor yang terpengaruh oleh perkembangan teknologi informasi dan komunikasi adalah Perbankan, yang telah melahirkan inovasi digital serta memberikan dampak efisien dan efektivitas yang luar biasa.¹

Perkembangan globalisasi informasi dewasa ini membawa pengaruh yang sangat besar bagi kehidupan manusia, perkembangan ini telah menyebabkan hubungan dunia menjadi tanpa batas yang juga berdampak pada perubahan sosial masyarakat secara signifikan.

Peradaban yang semakin modern ini sangat mempengaruhi perilaku orang dalam hidup bermasyarakat. Ilmu pengetahuan dan teknologi yang semakin canggih sehingga komunikasi menjadi semakin lancar dan semakin cepat terjadinya. Hadirnya internet ditengah masyarakat mempunyai pengaruh positif dan pengaruh negatif. Internet telah menjadi permasalahan khusus sejak dimanfaatkan dalam kegiatan perdagangan atau bisnis yang dikenal dengan transaksi *e-commerce*.²

Transaksi melalui internet bisa terjadi hanya dengan membuat kesepakatan atau kontrak yang dilakukan melalui media online. Kegiatan teknologi informasi dapat dimanfaatkan untuk penyebaran dan pencarian

¹ Resa Raditio, *Aspek Hukum Transaksi Elektronik*, (Jakarta: Graha Ilmu, 2014), hal. 65.

² Budi Agus Riswandi, *Hukum Dan Internet Di Indonesia*, (Yogyakarta: Uii Press, 2003), hal. 113.

data yang bermanfaat untuk berbagai kegiatan keseharian. Kegiatan ini tidak dapat berlangsung jika tidak didukung oleh suatu sistem telekomunikasi. Perkembangan teknologi informasi komunikasi berbasis komputer telah berkembang sangat pesat di masyarakat.³

Di Indonesia, penerapan layanan 5G secara komersial dimulai atau masuk ke Indonesia pada Mei 2021 lalu. Teknologi layanan 5G merupakan sebuah teknologi telekomunikasi baru yang sedang berkembang saat ini. Teknologi ini memiliki kecepatan internet hingga 10 Gbps. Angka ini jauh lebih tinggi dari kecepatan internet 4G yang hanya sebesar 100 Mbps. Dengan angka tersebut, pengguna dapat mengunduh film berdurasi lama hanya dalam beberapa detik saja. Namun penggunaan 5G tidak hanya sebatas mengunduh film, streaming video, ataupun bermain game online saja. Teknologi ini memiliki low latency (keterlambatan rendah) sehingga dapat dimanfaatkan di berbagai bidang seperti transportasi, sistem keamanan, kesehatan dan berbagai bidang lainnya.

Beberapa operator jasa layanan telekomunikasi di Indonesia sudah melakukan uji coba 5G. Operator tersebut, antara lain Telkomsel, XL, Indosat, dan Tri. Mendukung implementasi teknologi 5G, operator fokus dalam menyiapkan infrastruktur yang perlu dibangun untuk implementasi 5G. Operator akan menyanggupi penambahan teknologi 5G bila ekosistem penunjangnya sudah tersedia. Selain itu, operator juga menunggu regulasi pemerintah mengenai pemilihan spektrum frekuensi yang akan digunakan.

³ Leonardo Latsiano, Kajian Yuridis Tentang Tindak Pidana Penyebaran Data Pribadi Melalui Internet (Doxing) Di Indonesia, Jurnal Fakultas Hukum Universitas Sam Ratulangi Lex Privatum Vol.13 No.3 Feb 2024.

Sejauh ini, hanya pengguna layanan seluler di kota-kota besar yang dapat menikmati layanan 5G.⁴

Kementerian Komunikasi dan Informatika saat ini tengah menyiapkan insentif penerapan teknologi jaringan telekomunikasi 5G di Indonesia. Menteri Komunikasi dan Informatika Budi Arie Setiadi mengatakan hal ini merupakan langkah strategis dalam mengoptimalkan jaringan 5G guna meningkatkan kecepatan internet di Indonesia. Menteri Budi Arie meyakini kecepatan internet Indonesia akan terus tumbuh seiring berkembangnya teknologi digital. Menurutnya, Kementerian Kominfo selalu mengupayakan kecepatan internet Indonesia bisa masuk sepuluh besar dunia dengan bantuan jaringan 5G. Itu sebabnya pemerintah terus fokus pada penerapan infrastruktur digital. Guna menyediakan layanan jaringan Internet yang berkualitas, pemerintah terus memperhatikan dinamika industri dalam negeri. Menteri Komunikasi dan Informatika Budi Arie Setiadi juga merekomendasikan agar ekosistem industri meningkatkan kualitasnya secara sehat dan menjaga daya saing.⁵

Presensi revolusi digital dalam siklus penciptaan inovasi telah mendorong bagaimana teknologi dapat memperoleh, menyimpan, memanipulasi, hingga menstramisikan kompleksitas isi data secara menyeluruh dan real time. Berdasarkan hasil kajian perusahaan keamanan siber Surfshark, terdapat sekitar 1,04 juta akun di Indonesia yang mengalami

⁴ Ditra Andalisto, Yuliarman Saragih, Ibrahim, "Analisis Kualitatif Teknologi 5G Pengganti 4G Di Indonesia", JEE: Jurnal Edukasi Elektro, Vol. 06, No. 1, May 2022, hal. 4.

⁵ Sofyan Mufti Prasetyo, Rehan Gustiawan, Farhat, Fabian Rizzel Albani, "Analisis Pertumbuhan Pengguna Internet Di Indonesia", BIIKMA: Buletin Ilmiah Ilmu Komputer dan Multimedia, Vol. 2, No. 1 Juni 2024, hal. 67-69.

kebocoran data pribadi dalam jangka waktu kuartal II tahun 2022 dan jumlah tersebut melonjak hingga 143% dari kuartal I 2022.⁶ Tidak hanya itu, Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), jumlah pengguna Internet di Indonesia mencapai 221.563.479 jiwa pada tahun 2024, dari jumlah penduduk Indonesia sebesar 278.696.200 jiwa pada tahun 2023. Berdasarkan hasil Survei Penetrasi Internet Indonesia 2024 yang dipublikasikan oleh APJII, tingkat penetrasi internet-Net Indonesia meningkat sebesar 79,5%. Dibandingkan musim sebelumnya, peningkatannya sebesar 1,4%. Muhammad Arif saat mengumumkan hasil survei internet kantor APJII di Indonesia, penetrasi internet berdasarkan gender sebagian besar adalah laki-laki sebesar 50,7% dan perempuan sebesar 49,1%. Sedangkan yang berselancar di dunia maya mayoritas sebesar 34,40 persen merupakan Generasi Z (lahir 1997-2012). Kemudian generasi milenial (lahir 1981-1996) sebanyak 30,62%. Kelompok umur generasi penerus (lahir 1946-1964) sebesar 6,58% dan sebelum masa (lahir 1945 sebesar 0,24%). APJII menemukan wilayah perkotaan masih menjadi yang terbesar (69,5% dan perdesaan 30,5%) Dalam melakukan survei terhadap pengguna Internet di Indonesia, APJII mengikutsertakan konsultan Indektati melalui survei wawancara tatap muka. Metode ini diikuti oleh 8.720 responden dari 38 provinsi di Indonesia. Namun penelitian ini dilakukan pada 18 desember 2023 sampai 19 januari 2024. Namun metode

⁶ Vika Azkiya Dihni, "Kasus Kebocoran Data di Indonesia Melonjak 143% pada Kuartal II 2022," Databoks, 2022, diakses pada <https://databoks.katadata.co.id/datapublish/2022/08/09/kasus-kebocorandata-di-indonesia-melonjak-143-pada-kuartal-ii-2022>.

pengambilan sampelnya menggunakan sampel acak bertingkat dengan margin kesalahan 1,1% dan kesalahan standar relatif 0,43%.

Jumlah pengguna internet di dunia pada tahun 2024 sebanyak 5,35M atau setara 69,4% dari jumlah populasi di dunia sebanyak 8,08M orang. Data Reportal pada bulan Januari 2024 menyampaikan keadaan digital di Indonesia pada tahun 2024.



Gambar 1. 1 Data Reportal penggunaan data digital di Indonesia

Berikut ini adalah berita utama Data Reportal yang penting untuk adopsi dan penggunaan digital di Indonesia pada awal tahun 2024⁷:

1. Jumlah Populasi sebanyak 278,7 juta orang.
2. Terdapat 185,3 juta pengguna internet di Indonesia pada awal tahun 2024, dengan penetrasi internet mencapai 66,5 persen dari Total populasi.
3. Indonesia memiliki 139 juta pengguna media sosial pada Januari 2024, setara dengan 49,9 persen dari total populasi.

⁷ Simon Kemp, "Digital 2024: Indonesia". <https://datareportal.com/reports/digital-2024-indonesia>, diakses pada 5 September 2024.

4. Sebanyak 353,3 juta sambungan seluler aktif di Indonesia pada awal tahun 2024, atau setara dengan 126,8 persen dari total penduduk. Satu orang ada yang memiliki 2 atau lebih sambungan seluler aktif
5. Waktu yang dihabiskan dalam mengakses internet selama 7 jam 38 menit dalam sehari.
6. Waktu yang dihabiskan dalam mengakses media sosial selama 3 jam 11 menit.
7. Waktu yang dihabiskan untuk permainan (games) selama 1 jam 12 menit.
8. Alasan menggunakan internet yaitu Mencari informasi (83,1%), berkomunikasi dengan teman dan keluarga (70,9%), mencari ide dan inspirasi baru (70,6%), menelusur dan membagikan hal-hal yang umum (62,9%), mendapatkan/memperbaharui berita dan informasi terbaru (61,1%), menonton video, TV, pertunjukan, dan film (60,6%), akses dan mendengarkan musik (58,4%), penelitian mengerjakan sesuatu (48,8%), penelitian produk dan merek (46,1%), pertemuan dengan orang baru dan melakukan koneksi baru (41,1%), penelusuran tempat, lokasi dan wisata(40,8%), permainan (games) (40,3%), penelusuran bidang kesehatan dan produk kesehatan (39,1%), berbagi opini (37,4%), dan mengelola keuangan dan tabungan (36,0%).⁸

Teknologi informasi dan komunikasi telah melahirkan inovasi perbankan serta memberikan dampak efisien dan ektivitas yang luar biasa.

⁸ *Ibid.*

Salah satu inovasinya yaitu bank menciptakan produk dan jasa. Produk dan jasa yang dilakukan oleh bank harus sesuai dengan ketentuan yang ada berdasarkan jenis banknya sebagaimana yang diatur dalam Undang-Undang Nomor 7 tahun 1992 tentang perbankan sebagaimana telah diubah dengan Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan dalam ketentuan Pasal 1 angka 1 yang dimaksud dengan Bank adalah “badan usaha yang menghimpun dana dari masyarakat dalam bentuk simpanan, dan menyalurkannya kepada masyarakat dalam rangka meningkatkan taraf hidup rakyat banyak”. Bank merupakan “suatu lembaga keuangan tempat penyimpanan dana atau uang dari perusahaan-perusahaan, baik badan usaha besar, menengah maupun kecil, baik perorangan maupun lembaga, pemerintah maupun swasta”. Bank merupakan suatu lembaga yang sangat penting di dalam masyarakat, karena bank sebagai salah satu sarana berjalannya perekonomian yang ada di masyarakat.⁹

Pengertian bank dirumuskan di dalam Pasal 1 angka 2 sebagai berikut:
“Bank adalah badan usaha yang menghimpun dana dari masyarakat dalam bentuk simpanan dan menyalurkannya kepada masyarakat dalam bentuk kredit dan atau bentuk-bentuk lainnya dalam rangka meningkatkan taraf hidup rakyat banyak”

Cyber crime merupakan kejahatan di dunia maya. Salah satu jenis kejahatan yang meningkat di dunia modern yang serba online karena kemajuan teknologi. Berbagai macam jenis modus kejahatan *cyber crime*. Mulai dari meminta-minta sumbangan atas nama kemanusiaan, pencurian

⁹ Budi Agus, *Aspek Hukum Internet Banking*, (Jakarta: PT. Raja Grafindo Persada 2005), hal. 24.

data, sampai pembobolan rekening. *Cyber crime* termasuk perilaku ilegal yang dilakukan pelaku kejahatan dengan cara penggunaan teknologi komputer dan jaringan internet guna menyerang sistem informasi korban. Seperti melakukan hack media sosial, masuk dengan paksa pada perangkat teknologi dan data-data korban. Selanjutnya, merampas habis saldo rekening atau kartu kredit korban. Teknologi informasi dan komunikasi telah melahirkan inovasi perbankan serta memberikan dampak efisien dan ektivitas yang luar biasa. Salah satu inovasinya yaitu bank menciptakan produk dan jasa. Produk dan jasa yang dilakukan oleh bank harus sesuai dengan ketentuan yang ada berdasarkan jenis banknya sebagaimana yang diatur dalam Undang-Undang Nomor 7 tahun 1992 tentang perbankan sebagaimana telah diubah dengan Undang-Undang Nomor 10 Tahun 1998.¹⁰

Ada dua faktor yang dapat memicu munculnya *cybercrime*, yaitu faktor teknis dan faktor sosio-ekonomi. Secara teknis, perkembangan teknologi informasi dapat memiliki dampak negatif pada kemajuan masyarakat. Keberhasilan teknologi tersebut dapat menghilangkan batas-batas wilayah negara dan mempersempit dunia. Keterhubungan antar jaringan juga dapat memudahkan pelaku kejahatan untuk melakukan aktivitas kriminal. Selain itu, ketidakmerataan distribusi teknologi juga dapat menyebabkan ketimpangan kekuatan antara individu atau kelompok.

¹⁰ Muhammad Fikri, Shelvi Rusdiana, "Ruang Lingkup Pelindungan Data Pribadi: Kajian Hukum Posistif Indonesia", *Ganesha Law Review*, Vol. 5, No. 1 15 September 2023, hal. 76.

Pencurian data di dunia online dikenal dengan istilah phishing, yang merupakan kejahatan untuk memperoleh informasi pribadi atau rahasia seseorang secara ilegal. Tindakan ini bertujuan untuk memperoleh nomor kartu kredit, PIN, User ID, nomor telepon, nomor rekening, dan informasi pribadi lainnya.¹¹

Salah satu metode yang digunakan oleh pelaku phishing adalah dengan menyebarkan tautan palsu di akun media sosial melalui iklan yang menarik dan menggiurkan. Dengan cara ini, pelaku dapat mencuri informasi pribadi dari orang tersebut untuk mendapatkan keuntungan, misalnya dengan mencuri uang dari rekening pengguna atau menggunakan rekening tersebut sebagai media pembayaran online. Kejadian pelanggaran privasi yang melibatkan bocornya informasi pribadi sering terjadi di Indonesia.¹² Dalam sektor perbankan, informasi pribadi dapat terungkap dalam berbagai kegiatan seperti pertukaran data pribadi antara lembaga keuangan, penyaluran informasi kepada pihak ketiga terkait transaksi keuangan, atau melalui penyedia jasa pihak ketiga yang mengelola data transaksi. Di bidang medis, data pasien sering kali tersedia untuk tujuan asuransi atau program dukungan pemerintah tanpa persetujuan langsung dari pasien dan kadang-kadang dapat disalahgunakan untuk kepentingan yang tidak sah. Pada platform jual beli online, informasi pribadi seperti preferensi belanja dan riwayat transaksi sering kali diambil secara tidak sah menggunakan cookies

¹¹ Muhammad Fadli, Dijan Widijowati & Dwi Andayani, "Pencurian Data Pribadi di Dunia Maya (Phising Cybercrime) yang ditinjau dalam Perspektif Kriminologi", *Jurnal Ekonomi, Koperasi & Kewirausahaan*, Vol. 14, No. 12 Mei 2024, hal. 826.

¹² Disemadi H. S., & Prasetyo, "Tanda Tangan Elektronik pada Transaksi Jual Beli Online: Suatu Kajian Hukum Keamanan Data Konsumen di Indonesia." *Wajah Hukum*, Vol. 5, No. 1, April 2021, hal. 13–20.

yang dapat membahayakan privasi konsumen dan digunakan untuk kepentingan yang tidak diinginkan. Dalam platform transportasi online, penggunaan nomor telepon konsumen dapat disalahgunakan untuk tujuan yang tidak terkait dengan layanan, seperti mengirim pesan tidak relevan atau mengancam konsumen atas ulasan negatif.¹³

Pada tanggal 12 Mei 2021, Indonesia mengalami kasus serius terkait kebocoran informasi atau data pribadi yang melibatkan sekitar 279 juta data warga. Informasi yang tersedia mencakup detail seperti nama lengkap sesuai Kartu Tanda Penduduk (KTP), nomor telepon, alamat email, Nomor Identitas (NIK), lokasi tinggal, serta perkiraan pendapatan. Lebih dari 20 juta data juga dilengkapi dengan foto pribadi penduduk. Akun Kotz menawarkan sampel data gratis kepada pengguna dengan menyediakan 1 juta sampel dan memperkenalkan 3 tautan yang membutuhkan kata sandi untuk mengaksesnya. Kasus ini menimbulkan keprihatinan serius terhadap privasi data dan keamanan informasi pribadi masyarakat.¹⁴

Di balik kemudahan yang diperoleh dari penggunaan internet, ada juga resiko yang diperoleh ketika menggunakan layanan ini, diantaranya banyak terjadi pelanggaran hukum menyangkut data-data pribadi melalui internet dan juga mengenai resiko finansial yang diderita oleh penggunaan internet, terutama dalam hal ini adalah *internet banking*. Sementara ini, keamanan dan kenyamanan kurang diprioritaskan oleh banyak bank yang

¹³ Siti Yuniarti, "Pelindungan Hukum Data Pribadi di Indonesia", *Business Economic Communication and Social Sciences (BECOSS) Journal*, Vol. 1, No. 1 September 2019, hal. 149-151.

¹⁴ Luthiya, A. N., Irawan, B., & Yulia, R, "Kebijakan Hukum Pidana Terhadap Pengaturan Pencurian Data Pribadi Sebagai Penyalahgunaan Teknologi Komunikasi Dan Informasi", *Jurnal Hukum Pidana Dan Kriminologi*, Vol. 2, No. 2 Maret 2021, hal. 16-18.

masuk ke internet di Indonesia. Banyak nasabah bank yang tidak mau menggunakan fasilitas internet banking karena merasa tidak aman dan nyaman ketika melakukan transaksi.

Mayoritas nasabah merasa tidak aman jika web *internet banking* yang di akses adalah bukan web resmi melainkan manipulasi dari paracracker (*seam page*) dan juga takut ketika melakukan transaksi uang mereka tidak sampai ke tujuan yang disebabkan karena ulah para cracker. Bukan hanya itu, tetapi nasabah juga takut kalau PIN dan User ID mereka dapat diketahui oleh pihak yang tidak berwenang. Masalah tersebutlah yang membuat banyak nasabah tidak ingin menggunakan fasilitas internet banking, padahal fasilitas ini sangat efisien dan efektif. Hal ini juga dapat dikategorikan sebagai kebocoran data pribadi dari perusahaan perbankan.

Pada dasarnya Pelindungan hukum kepada nasabah merupakan hal yang sangat essential melihat adanya fungsi bank sebagai *agent of trust*. Bank sebagai agen of trust dengan dasar utama kegiatan perbankan adalah trust atau kepercayaan, baik dalam menyalurkan dana maupun dalam menghimpun dana. Besarnya kepercayaan nasabah terhadap sistem elektronik berkaitan dengan besarnya kepercayaan mereka terhadap online banking. Untuk mengatur adanya penggunaan teknologi informasi dalam dunia perbankan yang salah satunya internet banking, OJK membuat Peraturan Otoritas Jasa Keuangan No. 38/POJK.03/2016 tentang Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi oleh Bank

Umum (POJK Manajemen Resiko TI).¹⁵ Adanya pengaturan baik berupa undang-undang maupun peraturan Otoritas Jasa Keuangan diharapkan dapat mengakomodir semua kebutuhan Pelindungan hukum bagi nasabah yang akan melakukan transaksi internet banking.¹⁶

Namun ternyata peraturan ini masih terdapat tindakan yang melanggar hak-hak dan Pelindungan terhadap nasabah. Salah satu kasus terkait permasalahan internet banking adalah hilangnya uang nasabah pengguna internet banking. Pelindungan yang diberikan oleh bank sangat penting untuk menimbulkan kepercayaan dan kenyamanan nasabah. Karena resiko yang ditimbulkan dalam layanan ini sangat tinggi, ada kemungkinan nasabah menderita kerugian karena disadap oleh *hacker/cracker* yang mampu menembus firewall atau memasuki website yang memiliki nama domain yang hampir sama.¹⁷

Sangat terlihat jelas sekali dengan adanya kemajuan zaman dan teknologi yang semakin berkembang juga semakin mendukung tumbuh kembang kejahatan dunia maya (*cybercrime*) yang semakin bermacam-macam atau bisa disebut *cybercrime* yang berevolusi dan modus operadi yang berkaitan dengan tindakan kejahatan dunia maya. *Cyber crime* yang dulunya hanya dikenal dengan "*Hacking, Carding, Cracking*" hingga saat ini muncul berbagai macam bentuk kejahatan seperti "Denial of Service, Root Copromize (account compromixe dengan privilege bagi si penyusup),

¹⁵ Doni Purnama dan Rizki Anugrah. "Membangun Kepercayaan Nasabah Pada Internet Banking". *Ecodemica*, Vol. 3, No. 2 September 2015, hal. 465.

¹⁶ Gazali, Djoni S., and Rachmadi Usman. "*Banking Law*" Cet: III, Jakarta: Sinar Grafika, 2016, hal. 60.

¹⁷ Peter Mahmud, *Penemuan Hukum*, (Jakarta: Prenamedia Group, 2015), hal. 85.

Account Copromize (penggunaan akun secara ilegal), Probe (usaha untuk memperoleh akses ke dalam suatu sistem), Scan (Probe dalam jumlah besar), dan lain sebagainya.¹⁸

Yang justru menjadi persoalan bahwa adopsi teknologi terbaru, termasuk internet banking tidak bisa lepas dari proses edukasi kepada karyawan dan nasabah karena keduanya merupakan faktor yang berpengaruh terhadap transaksi. Realitas pembobolan rekening bank harus secepatnya dituntaskan demi menjaga reputasi internet banking. Pelindungan hukum berkaitan erat dengan rasa kepercayaan dan keamanan nasabah terhadap sistem tersebut, oleh karena itu diperlukan suatu Pelindungan hukum yang memadai.¹⁹

Jenis modus operadi berbasis teknologi yang semakin bervariasi dan berkembang dengan pesat ini mempunyai karakteristik tertentu yang membedakannya dengan kejahatan yang lain, diantaranya:²⁰

1. Kejahatannya berkaitan dengan teknologi yang bekerja secara elektronik dan sistem digital dibarengi dengan pendukungnya seperti data, program dan system.
2. Teknologi pada kejahatan ini mampu berposisi menjadi alat, sarana, objek, atau sasaran kejahatan , bahkan mungkin saja sebagai subjek kejahatan.

¹⁸ Barda Nawawi Arief, *Strategi Penanggulangan Kejahatan Telematika*, (Semarang, Uiniversitas Atma Jaya Yogyakarta, 2010), hal. 56.

¹⁹ Anggara, Bayu, and I. Nyoman Darmadha. "Penegakan Hukum Kejahatan Dunia Maya (Cybercrime) Yang Dilakukan Anak Di Bawah Umur", *Kertha Wicara: Journal Ilmu Hukum*, Vol. 5, No. 5 5 Mei 2016, hal. 47.

²⁰ *Ibid.*, hal. 68-70.

3. Perlakuan atau kegiatan itu dilakukan dengan ilegal, tanpa maksud tidak etis atau tanpa hak.
4. Perbuatan itu dilakukan dengan cara memanipulasi atau memperdaya teknologi hingga sebagaimana yang seharusnya (sesuai dengan kemauan pelaku).
5. Sifat kejahatan mengikuti sifat teknologi yang bersifat intangible, virtual, dan borderless.
6. Kerugian yang ditimbulkan tidak selalu bersifat material namun juga bersifat immaterial seperti privasi, keamanan, jasa, waktu, pelayanan).
7. Pelaku kejahatan via teknologi dilakukan oleh orang yang profesional dalam artian mempunyai pengetahuan dan keterampilan yang lebih di bidang pengembangan dan pemanfaatan teknologi.
8. Pelakunya susah untuk dicari sebab pada teknologi informasi, identitas seseorang dapat disamarkan secara sempurna.
9. Sebagaimana pelaku dunia Information Technology (IT) lainnya pelaku kejahatan via teknologi informasi juga mempunyai jiwa yang menyukai tantangan. Semakin terdorong untuk mencari celahnya atau kelemahannya dari sistem teknologi kemudian menyalahgunakan untuk motif-motif penyimpangan.
10. Korban kejahatan via IT ini umumnya tidak melaporkan kejahatan yang dialaminya, dengan beralasan tidak mengetahui kalau dirinya menjadi korban ketidakpercayaan pada aparaturnya penegak hukum atau takut terkena imbas yang lebih parah lagi.²¹

²¹ *Ibid.*

Semakin banyaknya kasus *cybercrime* (khususnya di Indonesia) telah menarik perhatian pemerintah untuk segera memberlakukan undang-undang yang dapat digunakan untuk menjebak pelaku kejahatan di dunia maya. Pemerintah Indonesia sendiri telah memasukkan UU *Cybercrime* (UU Siber) ke dalam UU ITE Nomor 19 Tahun 2016, dan berharap dengan adanya UU tersebut dapat mengatasi, mengurangi, dan menghentikan pelaku kejahatan di dunia maya.²²

Hukum berguna untuk menjadi payung hukum yang melindungi kepentingan masyarakat. Artinya hukum ada karena untuk melindungi segala bentuk kepentingan masyarakat di dalamnya agar terciptanya keadaan yang tenteram, aman dan damai.²³ Terdapat beberapa persoalan secara yuridis yang saling berkaitan dalam menjerat pelaku kejahatan *cyber crime* yakni, (1) siapa yang berhak mengatur atau membuat regulasi yang berhubungan dengan kejahatan di dunia maya jika melihat bahwasannya kejahatan ini melintasi batas teritorial atau bahkan bisa dilakukan diluar batas teritorial, yang berujung pada peradilan mana yang berhak mengadili kasus kejahatan ini. Tetapi dalam kajian ini lebih memfokuskan pada tindak kejahatan *cyber crime* teritorial nasional yang diatur pada Undang-Undang Nomor 19 Tahun 2016 atas perubahan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

²² Ade Arie Sam Indradi, *Carding: Modus Operandi, Penyidikan dan Penindakan*, (Jakarta: Grafika Indah, 2006), hal. 36.

²³ Astrini, Dwi Ayu. "Pelindungan Hukum Terhadap Nasabah Bank Pengguna Internet Banking Dari Ancaman *Cybercrime*." *Lex Privatum*, Vol. 3, No. 1 10 Ferbuari 2019, hal. 34.

Selanjutnya, (2) berkaitan dengan asas legalitas yang sangat mendasar dalam hukum pidana, apakah *cyber crime* mampu diikat dengan hukum pidana melalui cara interpretasi, mengingat tindakan jahat tersebut adalah suatu yang sama sekali baru. Sementara biasanya hukum pidana hanya menerima penafsiran otentik saja. Disamping berbagai persoalan lain yang kaitannya dengan seperti alat bukti elektronik dan sebagainya sebagai kelanjutan. Persoalan tersebut sebenarnya berkaitan dengan kebijakan hukum pidana. Marc Ancel mendefinisikan kebijakan hukum pidana sebagai suatu ilmu sekaligus seni yang bertujuan untuk memungkinkan peraturan hukum positif dirumuskan secara lebih baik.

Sementara itu upaya perumusan hukum pidana secara lebih baik, mencakup di dalamnya kebijakan merubah atau membuat aturan khusus (hukum pidana) yang berkaitan dengan kejahatan *cyber crime*.²⁴ Artinya walaupun secara essensial dapat di analogikan dengan kejahatan atau tindak pidana yang dapat diatur dalam Kitab Undang-Undang Hukum Pidana (KUHP), namun menurut pendapat para ahli, hukum pidana tidak menerima analogi. Disamping itu, juga karena karakteristik kejahatan tersebut yang berbeda maka dimungkinkan dijadikan tindak pidana tersendiri dengan aturan tersendiri pula dalam rangka mewujudkan rumusan hukum pidana yang lebih baik.

Kriminalisasi terhadap perbuatan-perbuatan yang dalam Bab VII sebagai perbuatan ada dua Undang- undang utama yang mengatur tentang

²⁴ Disemadi, Hari Sutra, and Paramita Prananingtyas. "Pelindungan Hukum Terhadap Nasabah Perbankan Pengguna CRM (Cash Recycling Machine)." *Jurnal Magister Hukum Udayana*, Vol. 8, No. 3 18 April 2019, hal. 87.

informasi dan transaksi elektronik di Indonesia. Undang-undang yang pertama adalah Undang-Undang Nomor 19 Tahun 2016 atas perubahan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Undang-undang yang ke dua adalah Undang-Undang No. 36 Tahun 1999 tentang Telekomunikasi. Kebijakan hukum pidana (*penal policy*) dengan membuat peraturan hukum pidana yang baik melalui pembaharuan hukum pidana materiel/ substantif, merupakan upaya yang dapat memberikan Pelindungan terhadap korban kejahatan *cyber crime* di bidang Informasi dan Transaksi Elektronik. Oleh karena itu, pembaharuan hukum pidana materiel atau substantif khususnya KUHP dalam rangka pembangunan/pembaharuan (sistem) hukum nasional merupakan kebutuhan penting dalam upaya memberikan Pelindungan terhadap masyarakat.²⁵

Dalam Konsep KUHP saat ini yang mempertegas pelaku kejahatan bukan hanya orang (*naturalijk person*), tetapi juga badan hukum (*recht person*) merupakan perkembangan yang sangat luar biasa, karena melalui pembaharuan KUHP terbuka kesempatan untuk memperluas jenis kejahatan yang juga dapat dilakukan oleh korporasi, yakni dengan memastikan atas perbuatan pidana siapa sajakah suatu korporasi harus bertanggung jawab secara pidana, serta menentukan jenis-jenis pidana yang paling tepat bagi korporasi agar dapat memberikan rasa adil bagi korban. Seiring perkembangannya, ternyata badan usaha atau korporasi tidak hanya bisa

²⁵ Nugraha, Ferry Satya, and Rinitami Njatrijani Budiharto. "Pelindungan Hukum Terhadap Nasabah Bank Dalam Pembobolan Internet Banking Melalui Metode Malware." *Diponegoro Law Journal*, Vol. 5, No. 3 3 Agustus 2016, hal. 89-90.

menjadi pelaku kejahatan *cyber crime* tetapi juga menjadi sasaran pelaku kejahatan dunia maya yang lain.²⁶

Sehubungan dengan hal-hal di atas, Pelindungan hukum amat sangat diperlukan bagi para nasabah pengguna *internet banking* yang bertujuan untuk melindungi hak-hak nasabah selaku konsumen dalam jasa perbankan, mengingat jasa hukum itu memandu dan melayani masyarakat. Kejahatan dunia maya ini di Indonesia telah diatur sebagaimana Undang-Undang Nomor 19 Tahun 2016 atas perubahan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Lalu konsep Pelindungan seperti apa yang tertuang dalam peraturan tersebut sehingga mampu melindungi nasabah, mengingat juga hukum itu memadu dan melayani masyarakat.

1.2 Rumusan Masalah

Mengacu pada latar belakang yang telah diuraikan sebelumnya, serta untuk memperjelas pembahasan yang akan dilakukan, beberapa isu pokok telah diidentifikasi. Dalam rangka memastikan fokus yang tepat dalam penelitian ini, maka penulis merumuskan beberapa permasalahan-permasalahan yang akan dibahas, sebagai berikut:

1. Bagaimana Pelindungan hukum terhadap data pribadi nasabah bank korban cyber crime dalam layanan perbankan digital?

²⁶ Sjahdeini, Sutan Remy, *Kejahatan dan Tindak Pidana Komputer*, (Jakarta: Pustaka Utama Grafiti, 2009), hal. 82.

2. Apa saja tantangan-tantangan dalam menegakkan Pelindungan hukum terhadap data pribadi nasabah bank korban cyber crime dalam layanan perbankan digital?

1.3 Tujuan Penelitian

Sebuah kajian ilmiah memerlukan tujuan yang terdefinisi dengan jelas sebagai panduan dalam pelaksanaan penelitian, serta sebagai penanda kualitas dari penelitian itu sendiri. Dengan merujuk pada permasalahan yang telah dirumuskan sebelumnya, tujuan yang ingin dicapai oleh penulis dalam penelitian ini dapat diuraikan sebagai berikut:

1. Untuk memecahkan persoalan hukum mengenai Pelindungan hukum terhadap data pribadi terhadap nasabah bank korban cyber crime dalam layanan perbankan digital.
2. Untuk memecahkan persoalan hukum mengenai tantangan dalam menegakkan Pelindungan hukum terhadap data pribadi nasabah bank korban cyber crime dalam layanan perbankan digital.

1.4 Manfaat Penelitian

1.4.1 Manfaat Teoritis

Penelitian ini diharapkan dapat menambah pengetahuan, baik bagi penulis maupun pembaca, serta dapat memberikan sumbangan pemikiran dalam perkembangan ilmu hukum, yang dalam penelitian ini khususnya mengenai Pelindungan hukum terhadap data pribadi nasabah nasabah bank korban cyber crime dalam layanan perbankan digital.

1.4.2 Manfaat Praktis

Penelitian ini diharapkan dapat memberikan manfaat bagi penulis, pembaca, serta nasabah terkait Pelindungan hukum terhadap data pribadi nasabah bank korban cyber crime dalam layanan perbankan digital. Selain itu, penelitian ini juga diharapkan dapat memberikan sumbangan pemikiran bagi aparat penegak hukum dalam menangani pelaksanaan Pelindungan hukum bagi nasabah atas terjadinya kejahatan cyber crime dalam layanan perbankan digital.

1.5 Sistematika Penulisan

Guna memudahkan dalam menguraikan pembahasan yang sistematis pada materi yang disajikannya tersebut, dengan ini peneliti melaksanakan penyusunan terhadap sistematika penulisan ini sebagaimana di bawah ini:

BAB I PENDAHULUAN

Dalam bab ini, akan dipaparkan secara ringkas isi dari bab-bab yang akan dibahas selanjutnya, yang kemudian akan diikuti dengan pembahasan tesis yang memiliki hubungan yang saling terkait untuk menyoroti tema utama topik ini. Bab ini juga bertujuan untuk menyajikan pembahasan secara sistematis yang dimulai dari latar belakang masalah penelitian, perumusan masalah penelitian, tujuan penelitian, manfaat penelitian, dan struktur penelitian yang akan diikuti.

BAB II TINJAUAN PUSTAKA

Pada tinjauan pustaka ini, terdapat dua aspek yang diperhatikan, yakni landasan teori dan landasan konseptual. Bagian landasan teori akan membahas berbagai teori yang relevan dengan penelitian, khususnya teori Perlindungan hukum dan teori kepastian hukum yang akan diuraikan dan diterapkan dalam konteks penelitian ini. Sedangkan, dalam landasan konseptual, akan dijelaskan definisi dan penjelasan kata-kata yang digunakan peneliti dalam menyusun tesis ini.

BAB III METODE PENELITIAN

Dalam bab metode penelitian hukum ini, peneliti akan menjelaskan tentang jenis penelitian yang dipilih, jenis data yang akan digunakan, teknik pengumpulan data yang akan diterapkan, pendekatan yang digunakan dalam menganalisis data, serta proses analisis data yang akan dilakukan.

BAB IV HASIL PENELITIAN DAN ANALISIS

Dalam bab ini, peneliti akan menguraikan jawaban atas permasalahan pada tesis ini, yaitu (i) melakukan analisa dan mendeskripsikan Pelindungan data pribadi terhadap nasabah bank korban cyber crime dalam layanan perbankan digital; (ii) menganalisis dan mengdeskripsikan penyelesaian Pelindungan hukum terhadap nasabah bank korban cyber crime dalam layanan perbankan digital.

BAB V PENUTUP

Bab ini merupakan bagian akhir yang mengemukakan rangkuman dari temuan dan analisis yang telah dibahas dalam bab-bab sebelumnya, serta memberikan rekomendasi dan saran untuk penelitian selanjutnya.

