BAB I

PENDAHULUAN

1.1. Latar Belakang

Kemajuan dan perubahan pesat dalam teknologi selama beberapa dekade terakhir mengubah aktivitas manusia, cara hidup dan cara menjalankan bisnis. Perkembangan internet dan telepon seluler telah membawa perubahan besar pada kebiasaan dan preferensi konsumen, yang mulai menggunakan media digital untuk berbagi informasi tentang diri mereka sendiri dan berkomunikasi dengan perusahaan, berbelanja online, dan menggunakan layanan internet baru.[1] Penyebaran secara global penggunaan internet dan seluler berkontribusi pada pengembangan bentuk baru pembayaran perbankan secara digital. Pembayaran digital diperkenalkan sebagai cara baru untuk melakukan transaksi keuangan yang nyaman dan efektif.[2] Pembayaran digital mengacu pada semua jenis pembayaran dengan menggunakan instrumen digital, yang meliputi pembayaran seluler, dompet seluler, *cryptocurrency*, dan pembayaran elektronik. Perbankan digital saat ini mengacu pada penggunaan teknologi digital dengan tujuan untuk melakukan transaksi perbankan dengan lebih lancar.[3] Oleh karena itu, istilah yang umum digunakan seperti perbankan elektronik (*e banking*), perbankan internet (*i banking*), dan perbankan online (*online banking*).

[1] Shareef, M. A., Dwivedi, Y. K., Kumar, V., & Kumar, U. (2017). Content Design Of Advertisement For Consumer Exposure: Mobile Marketing Through Short Messaging Service. International Journal Of Information Management, 37(4), 257–268.

[2] Leong, L. Y., Hew, T. S., Ooi, K. B., & Wei, J. (2019). Predicting Mobile Wallet Resistance:A Two-Staged Structural Equation Modeling-Artificial Neural Network Approach. International Journal Of Information Management, 102047.

[3] Sardana, V., & Singhania, S. Digital Technology In The Realm Of Banking: A Review Of Literature. Op Cit.

Senada dengan hal tersebut, Khan et al berpendapat bahwa perubahan teknologi yang meroket telah merevolusi lembaga keuangan menjadi digital; di sisi lain, nasabah perbankan menghadapi masalah karena masalah teknis dan kerahasiaan.[4] Adanya kemudahan melalui sarana digital perbankan membuat masyarakat semakin banyak yang mengakses untuk mendukung aktifitas kehidupan. Tidak diragukan lagi, industri perbankan saat ini melewati perkembangan pesat ditambah dengan inovasi teknologi yang menghasilkan peningkatan kehidupan finansial nasabah.[5] Selain itu, pandemi COVID-19 telah terbukti menjadi pembuka mata untuk pergeseran cepat ke format digital untuk transaksi perbankan. Rasionalisasi kebutuhan jam untuk penyediaan layanan perbankan digital yang lebih baik, Ahmed dan Sur[6] menganjurkan bahwa bank harus mengubah strategi mereka untuk mendorong transformasi digital mereka menuju ekonomi tanpa uang tunai.

Perbankan digital memerlukan penggunaan teknologi untuk memberikan layanan perbankan. Ini adalah istilah yang lebih luas daripada online atau mobile banking. Pada intinya, istilah "*going digital*" menunjukkan bahwa bank merangkul semua teknologi terbaru untuk operasi perbankan yang efisien.[7] Tidak hanya keuntungan yang diutamakan oleh pihak perbankan, namun dari sisi biaya juga diperhitungkan. Banyak lembaga perbankan fokus pada adopsi teknologi keuangan untuk transformasi digital perbankan, dimensi perubahan budaya memainkan peran

[4] I.U. Khan, Z. Hameed, S.U. Khan, Understanding Online Banking Adoption In A Developing Country: Utaut2 With Cultural Moderators, J. Global Inf. Manag. 25 (1) (2017) 43–65.

[5] S.J. Kaur, L. Ali, M.K. Hassan, M. Al-Emran, Adoption Of Digital Banking Channels In An Emerging Economy: Exploring The Role Of In-Branch Efforts, J. Financ. Serv. Market. 26 (2) (2021) 107–121.

[6] S. Ahmed, Sur, S. J. V.-X. J. O. M., Change In The Uses Pattern Of Digital Banking Services By Indian Rural Msmes During Demonetization And Covid-19 Pandemicrelated Restrictions, Vilakshan - Ximb J. Manag. (2021) 32.

[7] Wewege, L., & Thomsett, M. C. The Digital Banking Revolution. De Gruyter, (2009) 64.

penting dalam penyebaran dan adopsi teknologi baru, terutama di sektor perbankan.[8] Gelombang teknologi baru menciptakan persaingan yang sangat ketat dalam industri perbankan dimana yang bertransformasi dengan teknologi mutakhir akan lebih unggul karena dapat memenuhi kebutuhan pasar. Sayangnya, memahami warisan budaya nasabah yang mungkin memiliki dampak signifikan terhadap akseptabilitas perbankan digital merupakan tantangan besar bagi banyak institusi perbankan.[9]

Perbankan digital secara luas merupakan pergeseran paradigma menuju perbankan online di mana pelanggan dan bankir bergantung pada internet.[10] Perbankan tradisional terus bergeser ke format digital yang didukung oleh otomatisasi tingkat tinggi dan layanan berbasis *web* lainnya untuk memberikan transaksi keuangan. Perbankan digital menganggap bahwa nasabah bank memiliki internet, perangkat digital (misalnya, ponsel pintar, tablet, laptop, komputer pribadi) serta literasi digital yang memungkinkan mereka untuk mengelola layanan perbankan mereka sepanjang waktu.[11] Namun, terlepas dari hasil yang terlihat dari perbankan digital, ada beberapa mayarakat tetap kurang memanfaatkan layanan karena mereka membutuhkan berbagai jenis bantuan secara nyata. Mereka juga

[8] W.N. Picoto, I. Pinto, Cultural Impact On Mobile Banking Use–A Multi-Method Approach, J. Bus. Res. 124 (2021) 620–628.

[9] I.U. Khan, Z. Hameed, S.N. Khan, S.U. Khan, M.T. Khan, Exploring The Effects Of Culture On Acceptance Of Online Banking: A Comparative Study Of Pakistan And Turkey By Using The Extended Utaut Model, J. Internet Commer. (2021) 1–34, Https://Doi.Org/10.1080/15332861.2021.1882749.

[10] S. Ananda, S. Devesh, A.M. Al Lawati, What Factors Drive The Adoption Of Digital Banking? An Empirical Study From The Perspective Of Omani Retail Banking, J. Financ. Serv. Market. 25 (2020) 14–24.

[11] I.U. Khan, Z. Hameed, M. Hamayun, Investigating The Acceptance Of Electronic Banking In The Rural Areas Of Pakistan: An Application Of The Unified Model, Bus. Econ. Rev. 11 (3) (2019), Https://Doi.Org/10.22547/Ber/11.3.1.

merasa sangat membutuhkan dukungan teknis yang dapat meningkatkan kinerja mereka.[12]

Industri pembayaran yang menyerupai fitur perbankan memiliki pertumbuhan yang kuat selama dekade terakhir. Pasar pembayaran digital global bernilai USD 3885,57 miliar pada 2019 dan diperkirakan akan mencapai USD 8686,68 miliar pada 2025. Mr Ahmed Alenazi, Wakil Presiden, STC Pay menyatakan bahwa tingkat perubahan dalam industri pembayaran telah mempercepat karena berbagai alasan termasuk perubahan teknologi, adopsi internet dan penetrasi seluler di samping dorongan dan langkah pemerintah menuju masyarakat tanpa uang tunai.[13]

Meskipun penggunaan teknologi informasi secara ekstensif memungkinkan pelaksanaan bisnis yang semakin efisien, hal itu juga memperkenalkan serangkaian kerentanan baru. Hal ini menunjukkan bahwa industri keuangan merupakan sumber motivasi bagi pelaku kejahatan dalam melakukan kriminal.[14] Ketergantungan besar sektor keuangan pada teknologi informasi sebagai sarana untuk menjalankan bisnis, ditambah dengan segudang ancaman terhadap sistem teknologi dan informasi, menciptakan berbagai risiko terkait dunia maya di mana penjahat siap untuk menyelidiki dan mengeksploitasi potensi kerentanan dengan cara yang mudah. Karena sistem teknologi dan informasi menyediakan akses ke dana.[15] Teknologi menghubungkan ke berbagai data penting dan data rahasia. Singkatnya, dapat

[12] Khan, I. U. (2022). How Does Culture Influence Digital Banking? A Comparative Study Based On The Unified Model. Technology In Society, 68, 101822.

[13] Alkhowaiter, W. A. (2020). Digital Payment And Banking Adoption Research In Gulf Countries: A Systematic Literature Review. International Journal Of Information Management, 53, 102102.

[14] Varga, S., Brynielsson, J., & Franke, U. (2021). Cyber-Threat Perception And Risk Management In The Swedish Financial Sector. *Computers & Security*, *105*, 102239.

[15] Wilson, C., Kopp, E., & Kaffenberger, L. (2017). Cyber Risk, Market Failures, And Financial Stability (No. 2017/185). International Monetary Fund.

disimpulkan bahwa aktivitas terkait dunia maya, termasuk kejahatan dunia maya, menimbulkan risiko yang tidak dapat diabaikan bagi industri perbankan.[16]

Berbagai ancaman dunia maya mencakup segala hal mulai dari bencana alam, hingga ancaman yang melibatkan manusia. Cebula dan Young membagi tindakan yang dapat dilakukan orang untuk mengganggu sistem teknologi dan informasi menjadi tiga kategori: orang dapat (i) melakukan tindakan tidak disengaja, tanpa memiliki niat jahat atau berbahaya, misalnya, dengan melakukan kesalahan dan kelalaian, (ii) gagal mengambil tindakan dalam situasi tertentu, di mana tindakan sebaliknya akan mencegah hasil yang tidak diinginkan, atau (iii) bertindak dengan sengaja dengan maksud untuk menyakiti, misalnya dengan tindakan penipuan, sabotase, pencurian, dan vandalisme.

Tingkat ancaman *cyber* yang menargetkan korban secara acak sulit untuk ditentukan. Tidak ada kesepakatan tentang jenis insiden apa yang menyebabkan ancaman dunia maya dan apakah perilaku tertentu meningkatkan tingkat kejahatan.[17] Bahkan volume serangan *cyber* terhadap sektor mana pun, termasuk sektor keuangan, sangat sulit ditentukan. Secara tradisional, perusahaan cenderung tidak melaporkan insiden yang terkait dengan ancaman dunia maya untuk menghindari rasa malu dan kerusakan reputasi.[18]

Arti dari *cyber crime* atau kejahatan siber itu sendiri adalah "setiap jenis perilaku ilegal, tidak etis, dan tidak sah dalam suatu sistem yang memproses

[16] Varga, S., Brynielsson, J., & Franke, U. Cyber-Threat Perception And Risk Management In The Swedish Financial Sector. Op Cit

[17] Johnson, K. N. (2015). Cyber Risks: Emerging Risk Management Concerns For Financial Institutions. Ga. L. Rev., 50, 131.

[18] Varga, S., Brynielsson, J., & Franke, U. Cyber-Threat Perception And Risk Management In The Swedish Financial Sector. Op Cit.

informasi secara otomatis atau mentransfer data".[19] Pengertian tersebut menjelaskan bahwa dalam adanya perilaku illegal dalam suatu organisasi atau perusahaan akan mempengaruhi reputasi organisasi tersebut khususnya sektor keuangan/perbankan menjadi buruk. Kejahatan siber dengan sangat mudah menyebar dan berkembang di media sosial, karena media sosial menyediakan *platform* bagi penggunanya untuk berbicara tentang apa pun topik tanpa sensor atau kontrol yang diawasi.[20] Media sosial dapat menghadirkan ancaman baru bagi penggunanya karena potensi untuk mengakses sejumlah besar informasi pribadi yang diungkapkan oleh pengguna sosial media itu sendiri. Berbagai jenis aset rentan terhadap serangan di media sosial, termasuk informasi pribadi individu atau organisasi, identitas digital, aset keuangan, kekayaan intelektual, dan rahasia dan sumber daya perusahaan.[21] Di Indonesia permasalahan yang berkaitan dengan kejahatan siber khususnya dalam perbankan oleh pejabat Bank Indonesia dalam laporan *Financial Services Information Sharing and Analysis Center* menjelaskan bahwa Indonesia menjadi negara kesembilan dari sepuluh (10) negara yang memiliki angka *suseptibel* atau rentan akan kejahatan siber yang tinggi.[22]

Seiring dengan perkembangan teknologi di bidang informasi yang semakin cepat dan modern, menyebabkan sering terjadinya tindak pidana salah satunya pembuatan akun palsu yang dilakukan oleh seseorang, beberapa orang atau oknum

[19] Solak, D., & Topaloglu, M. (2015). The Perception Analysis Of Kejahatan sibers In View Of Computer Science Students. Procedia-Social And Behavioral Sciences, 182, 590-595.

[20] Goyal, S. (2012). Facebook, Twitter, Google+: Social Networking. International Journal Of Social Networking And Virtual Communities (Int J Socnet & Vircom),1 (1). 16-18.

[21] Fire, M., Goldschmidt, R., & Elovici, Y. (2014). Online Social Networks: Threats And Solutions. Ieee Communications Surveys And Tutorials, 16(4), 2019–2036. Https://Doi.Org/10.1109/Comst.2014.2321628

[22] Lidyana, V. (2020). Indonesia Masuk Daftar Negara Paling Rawan Kejahatan siber. 2020. Https://Finance.Detik.Com/Moneter/D-5248030/Indonesia-Masuk-Daftar-Negara-Paling-Rawan-Cyber-Crime

yang tidak bertanggung jawab. Pembuatan akun palsu atas nama seseorang tersebut dilakukan dengan berbagai tujuan khususnya di berbagai platform media sosial untuk melakukan kejahatan siber, misalnya mencari keuntungan dengan mengelabui korban, pembalasan dendam, penghinaan atau pencemaran nama baik, penyebaran konten-konten bermuatan kesusilaan, ujaran kebencian atau informasi kebohongan.[23] Dalam dunia perbankan, terdapat beberapa jenis kejahatan siber yang selama ini cenderung dilakukan oleh perorangan maupun kelompok pelaku, yaitu:[24]

1. Duplikasi atau Penggandaan Kartu.

   Misalnya: *skimming* ATM, pencurian nomor kartu kredit.
2. Nama Domain.

   Misalnya: calo / *cybersquat*, plesetan / *typosquating* nama domain, nama pesaing.
3. *Hijacking* atau Pembajakan (menggunakan komputer orang lain tanpa izin).
4. *Hacking* atau akses data tanpa izin (bisa dengan virus atau cara lain).
5. *Data leakage* atau membocorkan data, terutama data rahasia negara / perusahaan.
6. *Software piracy* atau pembajakan software terhadap hak cipta yang dilindungi HAKI.
7. *Hoax* atau pembuatan dan penyebaran berita palsu, dll.

[23] Markustianto, D., & Setiyanto, B. Tindak Pidana Pembuatan Akun Palsu Dalam Media Sosial Atas Nama Orang Lain (Studi Putusan Nomor: 10/Pid. Sus/2013. Pn. Pt). Jurnal Hukum Pidana Dan Penanggulangan Kejahatan, 8(1), 44-54.

[24] Junaedi, D. I. (2017). Antisipasi Dampak Penipuan rekayasa sosial Pada Bisnis Perbankan. Infoman's: Jurnal Ilmu-Ilmu Manajemen Dan Informatika, 11(1), 1-10.

Seiring dengan semakin canggihnya perlindungan sistem perbankan, hacker tidak hanya beroperasi di balik komputer untuk menyerang targetnya, tetapi mereka juga menghampiri targetnya secara langsung untuk mendapatkan informasi berharga yang mereka butuhkan sehingga dapat mengakses sistem yang terlindungi oleh benteng keamanan dan membuat penanganan keamanan apapun menjadi tidak berguna. Cara seperti itulah yang biasa disebut sebagai *social engineering* yang untuk kepentingan penelitian ini penulis menggunakan terminologi Penipuan Rekayasa Sosial.[25] Pelaku kriminal dunia maya sangat paham akan hal ini sehingga mereka menggunakan cara penipuan rekayasa sosial untuk mendapatkan informasi penting yang disimpan secara rahasia oleh manusia untuk tujuan tertentu.

Menurut Indrajit, "*social engineering* atau penipuan rekayasa sosial adalah suatu teknik atau informasi 'pencurian' atau pengambilan data atau informasi penting/krusial/rahasia dari seseorang dengan cara menggunakan pendekatan manusiawi melalui mekanisme interaksi sosial. Atau dengan kata lain penipuan rekayasa sosial adalah suatu teknik memperoleh data/informasi rahasia dengan cara mengeksploitasi kelemahan manusia". Dalam penipuan rekayasa sosial, si pelaku memanfaatkan sifat alamiah dari manusia. Hal ini diartikan bahwa betapa sifat alami manusia dapat diketahui dan dipelajari juga dimanfaatkan untuk tujuan tertentu. Banyak metode yang digunakan pelaku kejahatan dalam melancarkan usahanya agar bisa mendapatkan apa yang diinginkan. Biasanya dilakukan dengan cara memanfaatkan sisi psikologis seperti memuji, bersikap ramah, melakukan suatu hal yang berlebihan agar lebih dekat dengan targetnya seperti memberi

[25] Pada pelaksaannya di masyarakat menyebut modus kejahatan ini sebagai *social engineering*, tetapi dalam penelitian ini untuk mengindari ambiguitas terminilogi *social engineering* menurut Roscoe Pound maka digunakan istilah Penipuan Rekayasa Sosial.

sesuatu yang bisa membuat korban menjadi merasa senang dan bahagia, ataupun dengan cara membujuk. Banyak cara pelaku bisa mempermainkan emosi target sehingga tanpa sadar akan memberikan informasi rahasia.[26]

Dengan begitu, pelaku akhirnya bisa mengendalikan dan mendapatkan data pribadi sesorang. Pada kasus penipuan perbankan, praktik dari modus tersebut dilakukan oleh pelaku melalui panggilan telepon dan berpura-pura menjadi petugas bank. Nomor telepon yang digunakan pelaku biasanya mirip dengan nomor resmi sebuah perusahaan/institusi, plus memiliki kode area. Karenanya, tak sedikit nasabah terdorong untuk menjawab panggilan yang sebenarnya *fake caller number*. Saat panggilan diangkat oleh nasabah, oknum akan merekayasa cerita adanya aktivitas transaksi mencurigakan pada rekening atau kartu kredit dan menawarkan layanan pembatalan transaksi tersebut asal diberikan data pribadi. Adapun data perbankan pribadi yang diminta pelaku modus penipuan rekayasa sosial terdiri dari kode PIN, nomor kartu ATM, username, sekaligus PIN mobile banking, kode CVV, CVC kartu kredit, OTP yang diterima, serta informasi penting lainnya. Kepala Unit V sudit Kejahatan siber Polda Metro Jaya AKBP Dhany Aryandra mengatakan bahwa terdapat 2300 laporan masuk terkait penipuan aksi penipuan rekayasa sosial sepanjang tahun 2019. Bahkan, aksi tersebut menjadi kasus paling tinggi di antara lima tindakan kejahatan kejahatan siber lainnya yang rata-rata berjumlah 100 laporan per tahun.[27]

Penipuan rekayasa sosial berfokus pada mata rantai terlemah di dalam rantai kemanan informasi manusia. Kenyataannya, hampir semua solusi informasi sangat

[26] Junaedi, D. I. Antisipasi Dampak Penipuan rekayasa sosial Pada Bisnis Perbankan. Op Cit

[27] Https://Money.Kompas.Com/Read/2020/11/21/100100426/Sedang-Marak-Awasmodus-Pencurian-Data-Rahasia-Perbankan, diakses 25 Maret 2022.

bergantung pada manusia. Kelemahan ini bersifat universal, dan terbebas dari *hardware, software, platform*, jaringan, dan usia peralatan. Dalam hal membobol informasi, penipuan rekayasa sosial telah mencapai tingkatan tertinggi kematangan sebagai sebuah strategi. Keamanan ini digunakan perusahaan untuk melindungi apa yang dianggap asset-aset paling penting perusahaan, termasuk informasi. Mekanisme keamanan yang terbaik pun dapat ditembus dengan penipuan rekayasa sosial. Untuk mengurangi resiko tersebut, perbankan perlu untuk melatih dan mendidik staf dan pegawai mengenai ancaman keamanan dan bagaimana caranya mengenali serangan.[28]

Akan lebih mudah jika kita mengenali serangan untuk dapat menggagalkan sebuah serangan. Beberapa pertanda serangan penipuan rekayasa sosial yang dapat dikenali antara lain meminta informasi yang sifatnya pribadi dan rahasia, menolak memberi kontak, terburu-buru, mencatut nama, intimidasi dan hal-hal kecil seperti salah pengejaan nama atau pertanyaan agak aneh.

Kasus lain dari kejahatan siber dalam bentuk penipuan rekayasa sosial. Seperti yang dilakukan oleh Edward Snowden, seorang pegawai NSA, yang mencuri data dan membocorkannya, dengan menggunakan penyadapan yang dilakukan oleh NSA. Kasus penipuan rekayasa sosial terjadi pertama kali diluar negeri dilakukan oleh Kevin Mitnick. Kevin Mitnick adalah seorang pria Amerika Serikat yang di tahan di tahun 1995. Mitnick tercatat sebagai salah seorang hacker yang dalam mencari mangsanya hampir tidak menggunakan komputer dalam

[28] Junaedi, D. I. Antisipasi Dampak Penipuan rekayasa sosial Pada Bisnis Perbankan. Op Cit

mengeksploitasi kelemahan targetnya, dimana sebagian besar melakukan teknik penipuan rekayasa sosial.[29]

Kevin Mitnick telah menyatakan bahwa penipuan rekayasa sosial adalah bagian yang sederhana dalam pendekatannya. Bila rata-rata orang ingin melukisan bagaimana rupa hacker. Mitnick menyatakan dalam bukunya *The Art of Deception*, para pelaku penipuan rekayasa sosial merupakan hacker dengan keterampilan teknis tetapi ia memiliki keterampilan sosialisasi yang benar dan memanfaatkannya dalam memanipulasi orang, sehingga cara ini memungkinkan hacker untuk berbicara seperti biasa untuk mendapatkan data yang dinginkan secara tidak logis.[30]

Adapun kasus perbankan dalam negeri yang dilakukan oleh Steven Haryanto, membuat duplikasi situs asli tapi palsu di Bank BCA melalui internet BCA dan berharap agar nasabah masuk dalam situsnya terlihat nomor identitasnya dan nomor identifikasi nasabah. Dan ternyata terdapat 130 nasabah yang terperangkap oleh jebakannya. Sebagai contoh alamat palsu tersebut adalah: kilkbca.com, klikbac.com. Kemudahan dalam memperoleh informasi tersebut merupakan faktor kerentanan yang disebebkan oleh kelalaian manusia. Akibat dari kelalaian tersebut banyak perusahaan atau instansi yang dirugikan. Kerugian itu adalah hilangnya data informasi rahasia atau pencurian data yang memang harus di jaga.[31]

Pada kegiatan kerja sehari-hari budaya kerja karyawan masih tergolong kurang dalam disiplin pekerjaan. Pengetahuan tentang pentingnya keamanan informasi, mudah percaya kepada teman kerja dengan memberikan informasi,

[29]
[30] Ibid
[31] Ibid

masih adanya penekanan yang dilakukan oleh pejabat yang lebih tinggi jabatannya hal ini sangat rentan sekali terkait bagaimana menjaga kerahasiaan informasi yang dapat digunakan oleh para pelaku penipuan rekayasa sosial. Perilaku yang kurang baik ini dapat dimanfaatkan oleh pelaku penipuan rekayasa sosial. Misalnya *user* sebuah *system* menggunakan *password* yang mudah untuk dibobol, selanjutnya user tersebut tidak ingat untuk melakukan proses *logout* ketika meninggalkan ruang kerja. Hal tersebut akan memperbesar peluang pelaku penipuan rekayasa sosial untuk melakukan hal-hal yang illegal seperti mencuri informasi yang tidak seharusnya diketahui olehnya.

Penipuan rekayasa sosial merupakan salah satu metode di dalam peperangan asimetris. Hal ini dapat dibuktikan dengan adanya subjek yang lemah yaitu individu atau kelompok dan yang kuat yaitu sebuah perusahaan besar yang memiliki informasi rahasia. Penipuan rekayasa sosial juga merupakan salah satu cara dalam melakukan kejahatan siber, karena hal ini berkaitan dengan penerobosan pintu-pintu keamanan melalui sistem komputer.[32]

Seiring dengan semakin maraknya tindak kejahatan kejahatan siber di bidang perbankan yaitu kasus pembobolan terhadap sistem keamanan dan pembobolan rekening (*hacking*) atau sistem elektronik nasabah dalam sistem perbankan nasional dengan menggunakan sarana, prasarana dan identitas orang lain, sehingga dalam penegakan hukum pidana, korporasi khususnya lembaga perbankan tidak hanya menjadi korban pembobolan rekening nasabah tetapi juga masih bertanggung jawab atas kerugian yang dialami oleh nasabah.[33]

[32] Ibid

[33] Kusuma, M. J. (2013). Perlindungan Hukum Terhadap Nasabah Bank yang Menjadi Korban Kejahatan ITE di Bidang Perbankan. Al-Adl: Jurnal Hukum, 5(9).

Indonesia adalah salah satu penganut konsep negara hukum yang meterial yang mengadopsi konsep-konsep negara *welfare state*, dan secara implisit bisa dijumpai pada penjelasan umum UUD 1945, serta jika ditelisik secara keseluruhan isi dari UUD 1945 dapat ditarik keseimpulan bahwa negara Indonesia merupakan negara hukum yang material atau negara dengan konsep *welfare state* dimana negara mempunyai tanggungjawab mutlak untuk memajukan kesejahteraan umum dan mewujudkan keadilan sosial bagi seluruh warga negaranya.[34]

Spicker berpendapat bahwa *welfare state* dapat didefinisikan sebagai sebuah sistem kesejahteraan sosial yang memberi peran lebih besar kepada negara (pemerintah) untuk mengalokasikan sebagian dana publik demi menjamin terpenuhinya kebutuhan dasar warganya. Sementara, Husodo menyatakan bahwa negara kesejahteraan (*welfare state*) secara singkat didefinisikan sebagai suatu negara dimana pemerintahan negara dianggap bertanggung jawab dalam menjamin standar kesejahteraan hidup minimum bagi setiap warga negaranya.[35]

Menurut Esping-Anderson, *welfare state* pada dasarnya mengacu pada peran negara yang aktif dalam mengelola dan mengorganisasi perekonomian yang di dalamnya mencakup tanggung jawab negara untuk menjamin ketersediaan pelayanan kesejahteraan dasar dalam tingkat tertentu bagi warga negaranya. Secara umum suatu negara bisa digolongkan sebagai *welfare state* jika mempunyai empat pilar utamanya, yaitu: *(1) social citizenship; (2) full democracy; (3) modern industrial relation systems;* dan *(4) rights to education and the expansion of modern mass educations systems.* Keempat pilar ini dimungkinkan dalam negara

[34] Hadiyono, V. (2020). Indonesia dalam Menjawab Konsep Negara Welfare State dan Tantangannya. Jurnal Hukum, Politik dan Kekuasaan, 1.

[35] Sukmana, O. (2016). Konsep dan Desain Negara Kesejahteraan (Welfare State). Jurnal Sospol, 2(1), 103-122.

kesejahteraan karena negara memperlakukan penerapan kebijakan sosial sebagai penganugerahan hak-hak sosial (*the granting of social rights*) kepada warganya. Dalam garis besar, negara kesejahteraan menunjuk pada sebuah model ideal pembangunan yang difokuskan pada peningkatan kesejahteraan melalui pemberian peran yang lebih penting kepada negara dalam memberikan pelayanan sosial secara universal dan komprehensif kepada warganya.

Dalam kerangka negara hukum kesejahteraan (*welfare state*), negara memiliki keterlibatan dalam aspek kehidupan masyarakat. Guna peningkatan fungsi negara, negara secara langsung maupun tidak langsung melakuan aktivitas pengumpulan, pengolahan dan penyimpanan data pribadi warga negara. Di Indonesia pelanggaran terhadap penggunaan data pribadi kerap terjadi. Pada praktik perbankan, pertukaran data pribadi dilakukan melalui sistem sharing yaitu bertukar informasi tentang data pribadi nasabah di antara sesama *card center*, mengungkapkan informasi termasuk transaksi yang berhubungan dengan pemegang kartu kredit kepada pihak ketiga atau diperjual belikan di antara bank sendiri ataupun melalui pihak ketiga, yaitu baik perorangan maupun perusahaan-perusahaan pengumpul data serta memperjual belikan data pribadi nasabah.[36]

Sebagai negara hukum, Indonesia menjamin perlindungan atas hak asasi manusia dalam konstitusi negara. Sehingga dalam upaya melindungi masyarakat terkait pelanggaran terhadap penggunaan data pribadi pemerintah pada tanggal 21 April 2008 telah mengundangkan Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). Secara umum UU ITE dapat dibagi

[36] Yuniarti, S. (2019). Perlindungan hukum data pribadi di Indonesia. Business Economic, Communication, and Social Sciences (BECOSS) Journal, 1(1), 147-154.

dua bagian besar yaitu mengatur mengenai transaksi elektronik dan mengatur perbuatan yang dilarang *(cybercrimes).*[37]

UU ITE disahkan pada tahun 2008, kemudian pada tahun 2016 diubah secara terbatas, dengan cakupan undang-undang ini yang sifatnya “sapu jagad” (*one for all*) yang mengatur banyak hal yang terkait pemanfaatan teknologi informasi dan komunikasi, sejumlah materinya dianggap belum mampu merespon berbagai tantangan pemanfaatan dan perkembangan teknologi internet saat ini. Akibat format dan model pengaturan yang demikian, rumusan pengaturan yang disediakan oleh tiap pasalnya menjadi tidak mendetail dan mendalam, yang berdampak pada kelenturan dalam penafsiran serta implementasinya.

Dalam revisi UU ITE pada tahun 2016 yang lalu, dijelaskan dan ditegaskan bahwa untuk menjamin pengakuan serta penghormatan atas hak dan kebebasan orang lain dan untuk memenuhi tuntutan yang adil. Ada istilah "menjamin penghormatan dan hak kebebasan orang lain", tetapi kenyataannya masyarakat seolah diberangus dengan norma-norma di dalam UU ITE tersebut. Dengan kata lain, revisi tersebut tidak mengubah secara esensial persoalan yang ada di dalam UU ITE. Persoalan sesungguhnya ada pada masalah "kriminalisasi" dan "interpretasi norma". Pasal-pasal karet dan bermasalah serta multitafsir yang terdapat dalam UU ITE, telah memakan banyak korban. Namun dengan membuat sebuah pedoman interpretasi terhadap UU ITE belum cukup dan bukanlah langkah yang tepat untuk mengatasi permasalahan tersebut.

[37] Rohmy, A. M., Suratman, T., & Nihayaty, A. I. (2021). UU ITE Dalam Perspektif Perkembangan Teknologi Informasi dan Komunikasi. Dakwatuna: Jurnal Dakwah dan Komunikasi Islam, 7(2), 309-339.

Sejalan dengan hal tersebut, dalam permasalahan terkait dengan perbankan pada Surat Keputusan Bersama Nomor 229 Tahun 2021, Nomor 154 Tahun 2021, Nomor KB/2/VI/2021 tentang Pedoman Implementasi Atas Pasal Tertentu Dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) Pasal 28 ayat 1 point e menjelaskan bahwa Pasal 28 ayat 1 UU ITE merupakan delik materiil, sehingga kerugian konsumen sebagai akibat berita bohong harus dihitung dan ditentukan nilainya. Definisi "konsumen" pada Pasal 28 ayat (1) UU ITE mengacu pada Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen. Sehingga, berkaitan dengan pasal tersebut menjadikan perbankan tidak dapat melakukan pelaporan ke penegak hukum mengenai kasus yang dihadapi oleh nasabah.

Jika mempedomani SKB ini, maka dijelaskan bahwa pasal ini tidak dapat dikenakan pada pihak yang melakukan wanprestasi atau mengalami force majeur. Lalu, aturan ini merupakan delik materiil sehingga perlu ada kerugian konsumen sebagai akibat dari berita bohong. Kerugian itu harus terhitung dan ditentukan nilainya. Dari SKB UU ITE tersebut dapat ketahui bahwa media telepon tidak disebutkan secara tegas, sehingga kami berpendapat jika perbuatan pelaku penipuan tidak termasuk dalam unsur pasal UU ITE. Namun tidak menutup kemungkinan penegak hukum dapat mengenakan pasal berlapis terhadap suatu tindak pidana yang memenuhi unsur-unsur tindak pidana penipuan dan memenuhi unsur-unsur tindak pidana Pasal 28 ayat (1) UU ITE. Artinya, bila memang unsur-unsur tindak pidananya terpenuhi, penegak hukum dapat menggunakan pasal yang berkaitan dengan hal tersebut.

Pada pasal 36 disebutkan bahwa kerugian materiil terjadi pada korban orang perseorangan ataupun badan hukum, bukan kerugian tidak langsung, bukan berupa potensi kerugian, dan bukan pula kerugian yang bersifat non materiil. Secara keseluruhan, merujuk pada pelanggaran Pasal 27 hingga 34 yang kemudian mengakibatkan kerugian bagi orang lain. Pengusutan kasus sejenis ini merujuk pada kerugian langsung dan bukan berupa potensi kerugian. Sehingga, harus dihitung dan ditentukan nilainya. Dalam pedoman ini, nilai kerugian materiil merujuk pada Peraturan Mahkamah Agung (MA) Nomor 2 Tahun 2012 tentang Penyesuaian Batasan Tindak Pidana Ringan dan jumlah denda dalam KUHP lebih dari Rp 2,5 juta.

Sejalan dengan hal tersebut, Rohmy, dkk juga menyebutkan bahwa "beberapa persoalan terhadap UU ITE adalah Pasal 27 hingga Pasal 29 UU ITE dalam Bab Kejahatan Siber serta Pasal 26, Pasal 36, Pasal 40, dan Pasal 45". Persoalan yang terdapat di dalamnya adalah mengenai penafsiran hukum, dimana rumusan pasal-pasal dalam UU ITE tersebut tidak ketat (karet) dan tidak tepat serta menimbulkan adanya ketidakpastian hukum (multitafsir).[38]

Dari sisi perbankan sebagai bentuk tanggung jawab dalam memberikan perlindungan konsumen dan menjaga *trust issue* kepada nasabah terkait *kejahatan siber* khususnya modus *penipuan rekayasa sosial* diperlukan langkah-langkah preventif dan korektif guna mengoptimalkan upaya pencegahan tindak kejahatan perbankan di masyarakat. Angka jumlah korban tindak kejahatan perbankan semakin meningkat sehingga tidak hanya berdampak pada resiko financial baik nasabah maupun perusahaan tetapi juga resiko reputasi bagi perbankan itu sendiri.

[38] Rohmy, A. M., Suratman, T., & Nihayaty, A. I. UU ITE Dalam Perspektif Perkembangan Teknologi Informasi dan Komunikasi. Op Cit

Sebagai bentuk preventif, perbankan telah melakukan edukasi secara rutin tentang kewaspadaan tindak kejahatan perbankan melalui channel media sosial, media komunikasi *whatsapp blast*, *email blast* maupun melalui media konvensional radio. Namun demikian, diperlukan langkah lanjutan sebagai bentuk upaya hukum dan sekaligus untuk memberikan efek jera bagi oknum pelaku kejahatan siber khususnya dengan modus penipuan rekayasa sosial.

Berdasarkan uraian di atas, peneliti melakukan penelitian dengan judul **"PERLINDUNGAN HUKUM TERHADAP KEJAHATAN SIBER DENGAN MODUS PENIPUAN REKAYASA SOSIAL DALAM PRAKTEK PERBANKAN DI INDONESIA"**.

1.2. Rumusan Masalah

Dalam penelitian hukum ini akan muncul berbagai permasalahan yang beragam dan sangat luas. Oleh karena itu, untuk lebih mengkhususkan masalah pada penelitian ini, maka akan dibatasi dan difokuskan dengan mengidentifikasi masalah utamanya, yaitu:

a. Bagaimana pengaturan mengenai perlindungan hukum terhadap kejahatan siber dengan modus penipuan rekayasa sosial dalam praktek perbankan di Indonesia?
b. Bagaimana pelaksanaan perlindungan hukum terhadap kejahatan siber dengan modus penipuan rekayasa sosial dalam praktek perbankan di Indonesia?

1.3. Tujuan Penelitian

Sehubungan dengan apa yang telah dikemukakan dalam latar belakang dan perumusan masalah di atas, maka tujuan dari penelitian ini adalah:

a. Untuk mengetahui dan memahami penegakan hukum terhadap kejahatan siber dengan modus penipuan rekayasa sosial dalam praktek perbankan di Indonesia.
b. Untuk mengetahui bagaimana upaya penegakan hukum terhadap kejahatan siber dengan modus penipuan rekayasa sosial dalam praktek perbankan di Indonesia.

1.4. Manfaat Penelitian

Penelitian ini diharapkan dapat memberikan manfaat berupa:

a. Manfaat Teoritis
    a. Penelitian ini diharapkan dapat memberikan gambaran dan menambah pengetahuan mengenai penegakan hukum terhadap kejahatan siber dengan modus penipuan rekayasa sosial dalam praktek perbankan di Indonesia.
    b. Memberikan sumbangan pemikiran kepada pihak-pihak terkait dengan upaya penegakan hukum terhadap kejahatan siber dengan modus penipuan rekayasa sosial dalam praktek perbankan di Indonesia.
b. Manfaat Praktis
    1) Hasil penelitian ini diharapkan dapat memberikan informasi yang berupa bahan pertimbangan dalam menentukan kebijakan yang dipakai terkait dengan penegakan hukum terhadap kejahatan siber

dengan modus penipuan rekayasa sosial dalam praktek perbankan di Indonesia.

2) Penelitian ini diharapkan dapat dipergunakan sebagai sumbangan pemikiran mengenai upaya penegakan hukum kejahatan siber dengan modus penipuan rekayasa sosial dalam praktek perbankan di Indonesia yang bukan semata hanya untuk menanggulangi dan mencegahnya, namun lebih luas juga untuk menciptakan kondisi kehidupan masyarakat yang lebih aman.

1.5. Sistematika Penelitian

Susunan sistematika penulisan dari penelitian tesis ini disusun sebagai berikut:

(1) BAB I: Pendahuluan;

Bab ini akan menguraikan tentang latar belakang masalah, rumusan masalah, tujuan penelitian, manfaat penelitian dan sistematika penelitian.

(2) BAB II: Tinjauan Pustaka;

Pada bab ini diuraikan tentang kerangka teori yang berisi tinjauan kepustakaan yang menjadi literatur pendukung dalam pembahasan masalah penelitian.

(3) BAB III: Metodologi Penelitian

Pada bab ini diuraikan mengenai metodologi penelitian yang dilakukan dalam menyusun tesis ini, teori-teori yang menjadi landasan dilakukannya penelitian atas permasalahan yang timbul dan akan

dibahas. Bab ini juga akan membahas mengenai tata cara penelitian yang dilakukan untuk menghasilkan data mengenai bagaimana hambatan penegakan hukum terhadap kejahatan siber dengan modus penipuan rekayasa sosial dalam praktek perbankan di Indonesia.

(4) BAB IV: Pembahasan;

Pada bab ini diuraikan mengenai hasil penelitian atas hambatan penegakan hukum terhadap *kejahatan siber* dengan modus *penipuan rekayasa sosial* dalam praktek perbankan di Indonesia, termasuk juga tentang asas-asas yang harus dipenuhi, dengan menjawab pada rumusan permasalahan yang sudah diuraikan pada Bab I.

(5) BAB V: Penutup;

Pada bab ini akan disimpulkan secara ringkas mengenai pokok-pokok pembahasan dalam bentuk kesimpulan dan saran-saran yang mengacu pada hasil penelitian dan pembahasan yang telah diuraikan sebelumnya.