

BAB I

LATAR BELAKANG PEMILIHAN MASALAH HUKUM

Internet mengalami perkembangan yang luar biasa, hal ini dapat dilihat pada tahun 1998 yang diperkirakan lebih dari 100 juta orang yang tersambung ke internet dan jumlah ini meningkat dua kali lipat pada tahun 1999 dan diperkirakan akan lebih meningkat lagi pada tahun 2000an. Hal ini sudah terbukti, di Indonesia saja pada tahun 2016 jumlah pengguna internet sudah mencapai angka 132 juta (Bahri, 2020).

Kecanggihan teknologi disadari telah memberikan kemudahan, terutama dalam membantu pekerjaan manusia. Selain itu, perkembangan teknologi komputer menyebabkan munculnya kejahatan-kejahatan baru, yaitu dengan memanfaatkan komputer sebagai modus operasinya. Penyalahgunaan komputer dalam perkembangan menimbulkan persoalan yang sangat rumit, terutama kaitannya dengan proses pembuktian pidana (Maskun, 2013).

Kegiatan transaksi perbankan seperti penarikan dana, penyimpanan dana, transfer dana dan berbagai kegiatan transaksi perbankan lainnya. Kegiatan transaksi perdagangan dengan berbagai fasilitas seperti *e-commerce* dan e-bisnis, dimana transaksi *digital* telah menjadi sarana utama kegiatan bisnis ini. Kegiatan transaksi Pembayaran *online* yang telah digunakan oleh masyarakat untuk memenuhi kebutuhan pembayaran tagihan berbagai fasilitas yang ada dengan mudah dan efektif. Selain itu juga berbagai transaksi yang telah berubah menuju pada transaksi *e-money* sehingga individu dapat melakukan transaksi tanpa perlu menggunakan uang tunai lagi (Danuri, 2019).

Kecanggihan teknologi melalui media penjualan media masa yang digunakan sebagai transaksi ekonomi dapat memudahkan masyarakat mengakses suatu pelayanan dengan merancang suatu susunan berbisnis yang dengan mudah dengan langkah pengambilan keputusan dan sasaran yang tepat dalam melakukan transaksi ekonomi. Potensi besar dimiliki Indonesia dalam pengembangan ekonomi *digital*, sehingga berdampak signifikan terhadap perekonomian Indonesia. Jika kita melihat dampak utama pada sisi perkembangan ekonomi *digital* terdapat dua sisi dampak positif dan negatif dengan adanya teknologi dapat mempermudah seseorang dalam melakukan berbagai pelayanan.

Adanya jaringan komunikasi dalam transaksi ekonomi yang disalahgunakan dapat dengan mudahnya menimbulkan penipuan yang tak bertanggungjawab yang dapat merugikan banyak pihak baik dalam bentuk produksi maupun berbentuk keuangan yang membuat konsumen rugi besar. Penyalahgunaan komunikasi dapat berdampak pada norma, seperti adanya pencemaran nama baik dan sistem blokiran dan *hacker* pada sistem transaksi ekonomi (Maria & Widayati, 2020).

Hukum pidana merupakan suatu bidang hukum publik yang dimana menitikberatkan kepentingan umum atau kepentingan publik dalam proses pemidanaan. Penjatuhan pidana terhadap Tindakan *hacking* juga dapat dikenakan pada Pasal 378 KUHP jika *hacking* itu mengandung unsur penipuan dan bermaksud untuk menguntungkan diri sendiri menggunakan data orang lain (Putra W & abdurrachman H, 2023)

Cybercrime menurut Indra Safitri mengemukakan bahwa kejahatan dunia maya adalah jenis kejahatan yang berkaitan dengan pemanfaatan sebuah teknologi informasi tanpa batas serta memiliki karakteristik yang kuat dengan sebuah rekayasa teknologi yang mengandalkan kepada tingkat keamanan yang tinggi dan kredibilitas dari sebuah informasi yang disampaikan dan diakses pelanggan internet (Syarif Saddam Rivanie, 2020).

Keberadaan dunia *cyber* tersebut memberikan pengaruh yang besar terhadap berbagai bidang kehidupan. Namun pengaruh tersebut tidaklah selalu berdampak positif tetapi juga bisa berdampak negatif. Salah satu dampak negatif terwujudkan dengan adanya istilah yang dikenal dengan *cybercrime*. *Cybercrime* atau apabila yang diterjemahkan dalam bahasa Indonesia sebagai kejahatan dunia maya dapat mempunyai berbagai bentuk, misalnya seperti pemalsuan data, pencurian uang (*carding*), pornografi, perusakan *website* (*cracking*), hingga berbagai tindakan sejenis lainnya yang tidak diperbolehkan dalam peraturan perundang-undangan (Guntara, 2020)

Cybercrime seperti yang dimaksud ialah sebuah tindak kejahatan yang di lakukan dengan konsep kriminalitas yang menggunakan internet sebagai wahana kejahatan. Misalnya *carding* : mencuri kode PIN ATM milik orang lain buat di gunakan dalam transaksi *online* di internet, dan pemanfaatan media internet untuk menyebarkan alat-alat pembajakan. Pengirim *e-mail* anonim yang bermuatan iklan juga dapat dicantumkan dalam contoh kejahatan yang memanfaatkan internet sebagai medianya dan dapat dituntut dengan tuduhan pelanggaran privasi (Habibi & Liviani, 2020).

Sistem perbankan tidak dapat beroperasi tanpa dukungan teknologi informasi di era *digital* ini. Namun di sisi lain teknologi informasi memiliki dampak buruk juga pada sektor perbankan yaitu berupa kejahatan seperti *phishing*, *hacking*, pemalsuan, kecurangan adanya kebutuhan untuk mencegah kejahatan dunia maya dengan memastikan teknik otentifikasi, indentifikasi dan verifikasi ketika seseorang masuk ke segala jenis dunia maya dan kompleksitas prosedur investigasinya memerlukan langkah-langkah yang tepat untuk diadopsi, guna meningkatkan kerjasama antar pemangku kepentingan untuk menaggulangi kejahatan siber.

Kejahatan di bidang perbankan memiliki arti luas yaitu segala tindak pidana terkait perbankan seperti perampokan bank dan rekening yang dialihkan secara *illegal*. Sebaliknya kejahatan perbankan merupakan Tindakan yang dilarang dalam undang-undang seperti pendirian bank *illegal* dan rahasia bank yang dibocorkan (Iqbal et al., 2019).

Ragam kejahatan dalam aktifitas bisnis *e-banking* yaitu *hacking* yang mengancam *cyberspace* termasuk *e-banking* ialah *hacking* atau dalam Bahasa Indonesia disebut sebagai peretasan. Seiring meningkatnya pengguna internet semakin pesat juga perkembangan kejahatan *hacking*. Bos bank *central* asia sendiri, Jhaja Setiadamatja mengungkapkan bahayanya *hacking* bagi pengguna *e-banking*, nomor ini lah yang akan digunakan untuk mengirim kode OTP (*One Time Password*) kepada nasabah, masalahnya banyak nasabah yang sering mengganti nomor teleponnya, sehingga jika tidak berhati-hati nomor telepon yang lama dapat jatuh ke tangan yang salah. *Hacker* dapat menggunakan

nomor telepon tersebut untuk bertransaksi menggunakan *e-banking* dan kode OTP akan dikirim kepada *hacker* tersebut menyebabkan pembobolan akun *e-banking* (Ade Borami Ju et al., 2021).

Penipuan *online* didefinisikan menurut Mandelblit merujuk pada jenis penipuan dengan menggunakan media internet seperti ruangan *chat*, pesan elektronik, atau *website* dalam melakukan transaksi penipuan dengan media lembaga-lembaga keuangan seperti bank atau Lembaga lain yang berhubungan. Hal ini mendefinisikan bahwa penipuan *online* merupakan penipuan yang menggunakan perangkat lunak dan akses internet dalam melakukan tindakannya yang bertujuan untuk menguntungkan dirinya sendiri (Rahmad, 2019).

Keterkaitan antara Pasal 28 ayat 1 UU ITE dengan Pasal 378 KUHP dilihat dari unsur-unsur yang mengatur perbuatan terhadap Pasal tersebut. 28 ayat 1 Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik Tentang Perlindungan Konsumen, kaitan keduanya memiliki tujuan untuk meningkatkan kesadaran dan kemandirian konsumen untuk melindungi dirinya serta menciptakan perlindungan konsumen dengan memberikan kepastian hukum dan keterbukaan informasi serta akses untuk mendapatkan informasi (Sudin et al., 2022).

Terdakwa dengan sengaja dan maksud untuk mendapat keuntungan dengan menawarkan, membujuk atau mengiming-imingi dengan berinvestasi untuk memperoleh keuntungan yang besar hal tersebut mendorong seseorang

untuk menanamkan modalnya atau memberi sejumlah uang kepada terdakwa dengan harapan uang tersebut dalam waktu yang telah ditentukan memiliki jumlah yang semakin banyak, akan tetapi apa yang telah disepakati oleh terdakwa dan korban tidak sesuai dengan perjanjian investasi tersebut (Rahmawati & Dewi, 2020).

Berdasarkan analisis penulis majelis hakim mengatakan dalam kasus penipuan secara *online* terdapat unsur melawan hukum pidana karena terdapat unsur penipuan didalamnya. Untuk penipuan bisnis secara *online* ini pada prinsipnya sama dengan penipuan konvensional, yang membedakan hanya pada sarana perbuatannya yakni menggunakan sistem elektronik. Dalam kasus tentang diatas untuk penegakan hukum terhadap pelaku penipuan secara *online* ini dapat dikenakan Pasal 378 KUHP atau Pasal 45 ayat (2) Jo 28 Ayat (1) UU RI Nomor 19 Tahun 2016 tentang Perubahan atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Modus yang digunakan pelaku penipuan jual beli *online* adalah dengan mengajak pembeli bertransaksi di luar *marketplace* resmi dan menggunakan nomor rekening pribadi dari pelaku atau rekan pelaku untuk bertransaksi. Modus berikutnya adalah dengan berpura-pura mengatasnamakan *merchant online* dengan membuat situs palsu yang tujuannya adalah merekam *password* dan *username* calon pembeli yang untuk kemudian digunakan penipu untuk mengakses data-data lainnya, seperti nomor rekening dan riwayat transaksi perbankan. Modus berikutnya

adalah dengan pura-pura meminta *OTP* guna membobol rekening korbannya.

Mengenai perkara penipuan jual beli *online* yang ditangani oleh Subdit V *Cyber Crime* Ditreskrimsus Polda Jatim selalu menggunakan Pasal 28 ayat (1) UU ITE guna menjerat pelaku. Jika dilihat dari konstruksi hukum rumusan Pasal 28 ayat (1) UU ITE maka pada dasarnya pasal tersebut tidak menggunakan proposisi “penipuan” sebagaimana Pasal 378 KUHP yang jelas menggunakannya. Walaupun demikian, Pasal 28 ayat (1) UU ITE tetap dapat dijeratkan pada pelaku penipuan jual beli *online* dikarenakan kandungan proposisi ”berita bohong” dikarenakan penipu jual beli *online* selalu mengiklankan atau memasang penawaran penjualan barang baik di *web* atau *merchant online* yang dari stok barang, harga barang dan kewajiban pengiriman mengandung unsur “berita bohong” (Rantesalu, 2022).

Dalam hal ini didapati kasus penipuan *M-banking* terhadap kerabatnya namun tidak dilaporkan kepada kepolisian oleh korban karena tidak dapat keberanian dan juga kurangnya edukasi untuk melaporkan atas perbuatan tersebut,. Disamping itu faktanya tidak semua tindak pidana berujung kepada pemidanaan pelaku atau kasus tersebut tidak diproses secara hukum, salah satunya kasus penipuan *online* kasus tersebut sering ditemukan tetapi tidak adanya pelaporan kepada penegak hukum diantaranya dikarenakan beberapa alasan yaitu korban menganggap bahwa jika dilaporkan atau diproses secara

hukum akan menyita waktu, proses yang panjang hingga belum tentu yang menjadi kerugian akan kembali, korban tidak akan mendapat bantuan ketika melaporkan kasus dan kurangnya pengetahuan hukum yang baik untuk melaporkan kasus tersebut. Maka penulis tertarik mengangkat kasus diatas dengan memberikan pendapat hukum kepada korban terhadap kasus yang dialami.

Berdasarkan permasalahan di atas, penulis tertarik melakukan penelitian dalam bentuk memorandum hukum dengan judul **“PENDAPAT HUKUM TENTANG PERTANGGUNGJAWABAN HUKUM PIDANA TERHADAP PELAKU PENIPUAN *M-BANKING* DENGAN MODUS JUAL BELI *ONLINE* DALAM PERSPEKTIF CYBERCRIME”**