BAB I
PENDAHULUAN

A. Latar Belakang

Peningkatan pengguna teknologi informasi khususnya pengguna internet cukup signifikan, bahkan seolah-olah hal tersebut sudah menjadi suatu kebutuhan. Artinya individu dan kelompok yang tidak mampu beradaptasi dengan era virtual ini akan mengalami penurunan kemampuan kelangsungan hidup dan perkembangannya. Kita dapat melihat bahwa situasi saat ini bahkan akan menjadi aneh bagi seseorang yang tidak memiliki alat komunikasi. Perkembangan teknologi memberi arti positif menuju peradaban. Disertai dengan perkembangan internet, membuat banyak inovasi muncul di berbagai bidang kehidupan manusia, terutama dunia bisnis. Orang-orang sekarang percaya bahwa melalui Internet, pekerjaan dan kebutuhan mereka dapat dipenuhi secara efektif dan efisien. Salah satunya pada industri perbankan.

Industri perbankan memainkan peran yang sangat penting dalam perekonomian negara. Hal ini terlihat pada sektor perbankan yang terus berkembang. Perkembangan tersebut ditandai dengan meningkatnya volume transaksi yang dilakukan masyarakat, disertai dengan peningkatan risiko, kompleksitas transaksi, dan perkembangan teknologi di industri perbankan. Mereka bersaing dalam mendorong sektor perbankan dan non-perbankan untuk lebih inovatif dalam menawarkan berbagai alternatif layanan pembayaran, baik berupa sistem pengiriman uang maupun alat pembayaran menggunakan kartu elektronik, yang sederhana, cepat, efisien, dan global.

Bank Indonesia mencatat, nilai transaksi digital banking pada Oktober 2022 meningkat 38,38 persen dibandingkan dengan periode yang sama pada tahun sebelumnya manjadi Rp. 5.184,1 triliun (Merdeka.com, 2022). Pelaku industri perbankan tidak hanya perlu menerapkan teknologi digital, tetapi juga harus mampu menangkap peluang dengan lebih memahami perubahan perilaku konsumen yang semakin memimpin ranah digital untuk semakin memudahkan kebutuhan transaksi nasabah.

Menurut Ami Yusfalina Hutalgalung pada penelitiannya tahun 2020, masyarakat pada umumnya menginginkan transaksi yang cepat dan efektif tanpa perlu menghabiskan waktu untuk menunggu dan mengantre lama di bank. Kemudian dengan perkembangan teknologi terciptalah inovasi layanan yang bank berikan kepada nasabahnya yakni berupa *Mobile Banking* dan *Internet Banking*. Sedikitnya *mobile banking* dan *Internet Banking* tidak jauh berbeda perbedannya, yaitu sebuah fasilitas yang disediakan oleh suatu bank untuk memenuhi kebutuhan transaksi nasabahnya atau dengan kata lain *mobile banking* dan *Internet Banking* ini seperti mesin ATM namun tidak menerima atau mengeluarkan uang. Bedanya pada *mobile banking* adalah fasilitas berbasis aplikasi dan *Internet Banking* adalah fasilitas berbasis Web. Fasilitas ini berupa layanan pada transaksi perbankan dengan melalui jaringan internet, atau dapat disebut juga layanan bertransaksi dengan menggunakan *gadget* yang terhubung dengan jaringan internet tanpa perlu menjalankan aplikasi apapun.

Hadirnya layanan teknologi tersebut di industri perbankan memberikan banyak keleluasaan dan kemudahan dalam bertransaksi antara bank dengan nasabahnya, bank dengan *merchant*, bank dengan bank, dan nasabah dengan nasabahnya. Dalam perkembangan teknologi perbankan, sudah seharusnya bank memperhatikan aspek perlindungan untuk nasabahnya terlebih pada keamanan (*security*) yang berkaitan langsung dengan data pribadi nasabah.

وَٱلسَّارِقُ وَٱلسَّارِقَةُ فَٱقْطَعُوٓا۟ أَيْدِيَهُمَا جَزَآءًۢ بِمَا كَسَبَا نَكَٰلًا
مِّنَ ٱللَّهِ ۗ وَٱللَّهُ عَزِيزٌ حَكِيمٌ ﴿٣٨﴾

"Adapun laki-laki maupun perempuan yang mencuri, potonglah tangan keduanya (sebagai) balasan atas perbuatan yang mereka lakukan dan sebagai siksaan dari Allah. Dan Allah Maha Perkasa, Maha Bijaksana" Q.S Al-Maidah: 38

Pada ayat tersebut menjelaskan bahwa perbuatan mencuri termasuk dosa besar, oleh karena itu di dalam Islam pencuri akan dikenakan hukum potongan tangan dan wajib mengembalikan barang curian sebanyak yang dicuri. Dan seiring dengan berkembangnya teknologi macam-macam pencurian pun juga turut

mengiringi hal tersebut. Pesatnya perkembangan teknologi ini mengakibatkan kunjungan negatif dari para pengguna teknologi. Selain itu, risiko yang diperoleh melalui penggunaan teknologi termasuk banyaknya pelanggaran pencurian data pribadi melalui Internet, serta risiko keuangan kepada nasabah bank sebagai akibat dari tindakan pelanggar teknologi informasi. Kejahatan seperti ini juga sering disebut dengan *cyber crime*. Selanjutnya, para penjahat menggunakan teknologi informasi dan komputer yang canggih untuk melakukan tindak pidana pencucian uang dan terorisme. Dilihat dari berbagai peristiwa dalam beberapa tahun terakhir, Indonesia merupakan negara dengan *cyber security* lemah. Hal ini terlihat dari maraknya berbagai insiden, salah satunya yang terjadi pada akhir-akhir ini adalah bocornya data kartu debit nasabah bank melalui peretasan untuk menyusup ke sistem keamanan kartu nasabah dan kemudian tercatat sebagai citra buruk *cyber security* di Indonesia. Akibatnya banyak terjadi kejahatan, seperti untuk produk perbankan *online*, dan industri perbankan harus bisa menyediakan fitur keamanan yang menjaga tingkat kepercayaan nasabahnya terhadap keamanan transaksi elektronik.

Ancaman *cyber crime* di sektor perbangkan telah menjadi perhatian khusus terutama bagi nasabah. Tercatat ada 5.000 laporan pengaduan tindak penipuan (*fraud*) yang masuk ke website Kemkominfo setiap Minggunya. Sejak Maret 2020 hingga saat ini, hampir 200.000 laporan *fraud* telah diterima, paling banyak media yang digunakan adalah *WhatsApp* dan *Instagram* (Republika, 2021).

Selain laporan dari Kementerian KOMINFO, OJK juga tidak pernah bosan dalam mengingatkan masyarakat, untuk selalu waspada terhadap penawaran yang disampaikan melalui media termasuk media social atau aplikasi perpesan di dunia perbankan. Hingga 16 Juni 2022, OJK mencatat telah menerima 433 laporan *fraud*, dari total keseluruhan pengaduan yng sebanyak hampir 6000 laporan (Insight, 2022).

Dari sini, terdapat beberapa asumsi terkait masalah terbesar yang dihadapi bank saat ini. Pertama aplikasi pihak ketiga *smartphone* dan tablet kemungkinan memiliki keamanan yang lemah jika dibuat oleh pengembang yang tidak berpengalaman. Kedua jaringan *WiFi* publik yang merupakan salah satu cara

mudah bagi peretas untuk mendapatkan akses data ke berbagai informasi akun yang tersimpan pada *smartphone* penggunaannya. Ketiga ancaman *mobile malware*, 2*mobile malware* adalah perangkat lunak (*software*) berbahaya yang menyerang perangkat *Mobile* seperti *smart phone* maupun tablet yang tujuannya untuk merusak sistem operasi atau aplikasi dan/atau mencuri data pribadi maupun data perbankan. Pada kasus ini *mobile mallware* seperti virus, *Trojan*, *rootkit* dan lain lain, akan terus berkembang mengikuti perkembangan industri yang terus berkembang juga. Selain ancaman *mobile malware*, terdapat ancaman *mobile devices*, *digital connectivity*, *partnership*, API pada industri perbankan saat ini menjadi ancaman cyber crime (Republika, 2021).

Selain ancaman yang menyerang perangkat lunak *Smartphone* atau tablet. Modus *cyber crime* lainnya yang terjadi di sektor perbangkan meliputi *hacking* (peretasan), *skimming* (Penyalinan informasi), *defacing* (pergantian atau modifikasi halaman Web), *Phising* (pengelabuan), BEC (*business email compromise*) penipuan yang menargetkan para manajer keuangan perusahaan untuk melakukan pembayaran transfer secara legal dengan menyamar sebagai orang dari perusahaan.

Lebih dari 5000 laporan pengaduan tindak penipuan yang masuk sejak Maret 2020, *social engineering* (rekayasa sosial) adalah modus yang paling sering digunakan sepanjang tahun ini. Rekayasa sosial biasanya terjadi pada saat korban kurang waspada sehingga terpedaya memberikan data pribadinya seperti PIN atau *password* yang menjadikan pelaku kejahatan bisa mengakses akun dan mengambil alih nasabah di bank (CNBC Indonesia, 2021).

Pihak bank diharuskan untuk melindungi dan memperketat keamanan data transaksi nasabahnya dari kejahatan IT (*cyber*) supaya data nasabah yang menggunakan teknologi ini tidak mudah bocor atau diretas oleh para peretas atau pelaku kejahatan IT (*cyber*). Semakin mudahnya nasabah dalam mengakses produk dan layanan *Mobile Banking* dan *Internet Banking*, semakin banyak juga risiko *cyber crime* seperti *carding*, *hacking*, ataupun *cracking*, Dari hal tersebut, bank harus bisa menjanga keamanan produk dan layanan *online* sebagai langkah antisipasi dari dampak yang ditimbulkan oleh *cyber crime* yang belum maksimal diberikan pihak bank. Selain itu aspek penyampaian informasi produk perbankan

sebaiknya disampaikan secara proporsional, artinya bank tidak hanya menginformasikan keunggulan atau citra produknya saja, tapi juga harus menginformasikan sistem keamanan produk yang nantinya digunakan oleh si calon nasabah saat menawarkan (Hutagalung, 2020:3).

Oleh karena itu, berdasarkan uraian diatas penulis tertarik untuk melakukan penelitian tentang "**Pengaruh *Cyber Crime, Cyber Law* dan *Cyber Security* Terhadap Kepercayaan Nasabah Pengguna *Mobile Banking* dan *Internet Banking* (Studi Kasus: Mahasiswa Universitas Muhammadiyah Yogyakarta Nasabah BSI)**"

B. Rumusan Masalah

Dari uraian latar belakang diatas, maka penulis merumuskan beberapa pertanyaan seputar masalah yang terkait.

1) Apakah *cyber crime* berpengaruh negatif signifikan terhadap kepercayaan nasabah yang menggunakan *mobile banking* dan *internet banking*?
2) Apakah *cyber law* berpengaruh positif signifikan terhadap kepercayaan nasabah yang menggunakan *mobile banking* dan *internet banking*?
3) Apakah *cyber security* berpengaruh positif signifikan terhadap kepercayaan nasabah yang menggunakan *mobile banking* dan *internet banking*?
4) Apakah *Cyber Crime*, *Cyber Law*, dan *Cyber Security* berpengaruh terhadap Kepercayaan nasabah pengguna *mobile banking* dan *internet banking* secara bersamaan?

C. Tujuan Penelitian

Berdasarkan latar belakang dan rumusan masalah diatas, terbentuklah tujuan dari penelitian ini, yaitu sebagai berikut:

1) Untuk mengetahui apakah *cyber crime* berpengaruh negatif signifikan atau tidak berpengaruh negatife signifikan terhadap kepercayaan nasabah yang menggunakan *mobile banking* dan *internet banking*.

2) Untuk mengetahui apakah *cyber law* berpengaruh positif signifikan atau tidakberpengaruh positif signifikan terhadap kepercayaan nasabah yang menggunakan *mobile banking* dan *internet banking.*
3) Untuk mengetahui apakah *cyber security* berpengaruh positif signifikan atau tidak berpengaruh positif terhadap kepercayaan nasabah yang menggunakan *mobile banking* dan *internet banking.*

D. Manfaat Penelitian

Dari rumusan masalah yang dibetuk penulis serta tujuan penelitian tersebut, maka penelitian ini memiliki manfaat yakni sebagai berikut:

1) Manfaat Praktis

Hasil penelitian ini diharapkan nantinya dapat menjadi saran dan masukan terhadap pihak manajemen pemasaran Bank Syariah Indonesia mengenai pentingnya menangani masalah *Cyber Crime*, dengan memberi perlindungan bagi nasabah-nasabahnya dibawah peraturan perundang-undangan yang berlaku. Dan memperketat keamanan system untuk melindungi nasabahnya, untuk meningkatkan kepercayaan nasabahnya. Selain itu penelitian ini juga diharapkan dapat menyempurnakan manajemen yang masih kurang serta mempertahankan yang sudah baik.

2) Manfaat Teoritis

Harapannya penelitian ini dapat menjadi manfaat bagi pembaca yakni sebagai acuan dan referensi untuk penelitian selanjutnya. Tidak hanya itu, penelitian ini juga diharapkan dapat menambah wawasan bagi peneliti dan pembaca tentang perbankan syariah, terkhusus pada perilaku konsumen dan manajemen pemasaran.