BAB IV

ANALISIS PERATURAN DAN PENERAPAN MANAJEMEN RISIKO LAYANAN PERBANKAN ELEKTRONIK DAN PRINSIP PERTANGGUNGJAWABAN BANK XYZ ATAS KERUGIAN NASABAH AKIBAT PENIPUAN *SIM SWAP*

A. Analisis Pengaturan Terkait Manajemen Risiko Layanan Perbankan Elektronik dan Prinsip Pertanggung Jawaban Bank

Berdasarkan penelitian penulis, POJK MRTI sudah menjadi peraturan yang preventif dalam menangani risiko dalam penggunaan layanan perbankan elektronik oleh bank. Dibuktikan dengan mewajibkan bank menerapkan manajemen risiko sebagaimana diatur Pasal 2 ayat (2) POJK MRTI mencakup:

1. pengawasan aktif direksi dan dewan komisaris
2. kecukupan kebijakan, standar, prosedur penggunaan teknologi informasi
3. kecukupan proses identifikasi, pengukuran, pemantauan, dan pengendalian risiko penggunaan teknologi informasi
4. sistem pengendalian intern atas penggunaan teknologi informasi.

Penulis menemukan bahwa POJK MRTI belum memiliki pengertian mengenai apa itu risiko penggunaan teknologi informasi dan manajemen risiko penggunaan teknologi informasi oleh bank, akan tetapi pengertian risiko dan manajemen risiko yang umum telah ada dalam POJK MR.

Menurut Ikatan Bankir Indonesia, dalam menerapkan manajemen risiko bank perlu melaksanakan tata kelola manajemen risiko melalui pengawasan aktif dewan komisaris, direksi, dan manajemen senior bank lainnya.

Penulis menemukan bahwa Pasal 4 POJK MRTI telah mengatur mengenai kewajiban penerapan tata kelola tersebut. Lebih jelas diatur dalam Pasal 5 POJK MRTI mengenai bentuk pengawasan yang harus dilakukan direksi dan Pasal 6 POJK MRTI mengenai bentuk pengawasan yang harus dilakukan dewan komisaris dalam penggunaan teknologi informasi termasuk layanan perbankan elektronik oleh bank. Maka dari itu POJK MRTI telah cukup mengatur pengawasan direksi dan dewan komisaris dalam penerapan manajemen risiko layanan perbankan elektronik.

Menurut Ikatan Bankir Indonesia, selain menerapkan pengawasan aktif direksi dan dewan komisaris, bank juga perlu menyediakan kerangka manajemen risiko yang memadai dengan menyediakan kebijakan, standar dan prosedur yang cukup, Pasal 8 ayat (1) POJK MRTI telah mengatur hal tersebut yang dalam Pasal 8 ayat (2) disebutkan kebijakan, standar, dan prosedur yang dimaksud termasuk aspek layanan perbankan elektronik.

Akan tetapi POJK MRTI belum mengatur secara kompleks kecukupan kebijakan, standar dan prosedur manajemen risiko layanan perbankan elektronik, POJK MRTI hanya mengatur secara umum bahwa bank wajib menerapkan kebijakan, standar, dan prosedur penggunaan tekologi informasi oleh bank.

Ikatan Bankir Indonesia juga menyebutkan bank perlu menetapkan limit risiko yang telah diatur dalam Pasal 8 ayat (3) POJK MRTI yang mengharuskan

bank menetapkan limit risiko yang dapat ditoleransi dalam aspek terkait teknologi informasi termasuk layanan perbankan elektronik.

Selain itu, kerangka manajemen risiko juga termasuk menyediakan sistem organisasi manajemen risiko. Dalam manajemen risiko layanan perbankan elektronik yang diatur POJK MRTI, komite pengarah teknologi informasi adalah organisasi manajemen risiko penting yang ada di bawah direksi dan khusus membantu direksi dalam pelaksanaan manajemen risiko layanan perbankan elektronik dan penggunaan teknologi informasi oleh bank. Pengaturan komite pengarah teknologi informasi menurut penulis sudah cukup karena Pasal 7 ayat (1) dan (2) POJK MRTI telah mengatur secara jelas tugas dan tanggung jawab komite pengarah teknologi informasi.

Proses manajemen risiko terdiri dari identifikasi, pengukuran, pemantauan, dan pengendalian risiko. POJK MRTI telah mengatur kewajjiban bank melaksanakan proses tersebut dalam Pasal 10 ayat (2) POJK MRTI, dan proses manajemen risiko layanan perbankan elektronik secara rinci telah diatur dalam SEOJK MRTI. Akan tetapi proses identifikasi risiko layanan perbankan elektronik belum diatur dalam SEOJK MRTI, hanya diatur mengenai proses pengukuran, pemantauan, dan pengendalian manajemen risiko layanan perbankan elektronik.

Kewajiban bank untuk menerapkan prinsip pengendalian pengamanan data nasabah dan transaksi layanan perbankan elektronik telah diatur Pasal 29 POJK MRTI, prinsip tersebut adalah dasar dari peraturan pengendalian risiko layanan perbankan elektronik sebagaimana diatur SEOJK MRTI.

Ikatan Bankir Indonesia menyebutkan untuk memastikan seluruh jajaran organisasi melaksanakan kebijakan manajemen risiko yang sudah ditetapkan, bank memerlukan sistem pengendalian intern yang secara efektif mengawasi pelaksanaan kegiatan usaha dan operasional pada seluruh jenjang organisasi bank.

Pasal 17 ayat (1) POJK MRTI telah mengatur kewajiban bank melaksanakan sistem pengendalian intern atas penggunaan teknologi informasi dan cakupan pelaksanaan sistem pengendalian intern diatur dalam Pasal 17 ayat (2) POJK MRTI.

Berdasarkan penelitian, penulis mendapatkan gambaran bahwa POJK MRTI sudah menjadi peraturan yang represif melalui Pasal 36 POJK MRTI di mana bank yang tidak menerapkan manajemen risiko sebagaimana diatur POJK MRTI dapat diberi sanksi berupa:

a. Teguran tertulis;
b. Penurunan tangkat kesehatan berupa penurunan peringkat faktor tata kelola dalam penilaian tingkat kesehatan bank;
c. Larangan untuk menerbitkan produk atau melaksanakan aktivitas baru;
d. Pembekuan kegiatan usaha tertentu; dan/atau
e. Pencantuman anggota direksi, dewan komisaris, dan pejabat eksekutif dalam daftar tidak lulus melalui mekanisme penilaian kemampuan dan kepatutan.

POJK MRTI sudah menjadi peraturan yang memenuhi kewajiban bank sebagai pelaku usaha untuk beritikad baik sebagaimana daitur Pasal 7 huruf a

UUPK. Karena POJK MRTI mewajibkan bank menerapkan sistem layanan perbankan elektronik yang baik mulai dari adanya pengawasan direksi dan dewan komisaris; memiliki dan menerapkan kebijakan, standar, prosedur penggunaan teknologi informasi; memiliki dan menerapkan proses identifikasi, pengukuran, pemantauan, dan pengendalian risiko penggunaan teknologi informasi; dan memiliki sistem pengendalian intern atas penggunaan teknologi informasi.

Selain itu, POJK MRTI juga telah menjadi peraturan yang memenuhi kewajiban bank untuk menjaga keamanan simpanan, dana, atau aset nasabah yang berada dalam tanggung jawab bank karena POJK MRTI mewajibkan bank menjaga keamanan sistem melalui manajemen risiko layanan perbankan eletronik sehingga tidak mudah dibobol maupun terjadi kesalahan sistem yang dapat mengakibatkan hilangnya simpanan, dana, atau aset tersebut.

POJK MRTI telah menjadi peraturan yang memenuhi hak konsumen yaitu keamanan dalam mengkonsumsi jasa sebagaimana diatur Pasal 4 huruf a UUPK karena POJK MRTI mewajibkan bank menerapkan manajemen risiko untuk keamanan layanan perbankan elektronik.

Kewajiban bank untuk mengganti kerugian nasabah yang diatur Pasal 29 POJK PKJK menganut prinsip pertanggungjawaban *strict liability*. Hal ini penulis simpulkan dari penuturan Mudo Laksito yang menyatakan bahwa pertanggungjawaban bank tidak terbatas pada isi Pasal 29 POJK PKJK saja, karena bank juga wajib bertanggungjawab atas kerugian nasabah yang disebabkan pihak ketiga yang tidak berkaitan dengan bank.

Jadi, pertanggungjawaban bank menurut aturan tersebut dapat diperluas, tidak terbatas kepada kesalahan dan/atau kelalaian pengurus, pegawai bank, maupun pihak ketiga yang bekerja untuk kepentingan bank. Akan tetapi, bank juga bertanggung jawab kepada kerugian nasabah akibat perbuatan pihak ketiga yang melakukan penipuan *sim swap.*

Idealnya prinsip pertanggungjawaban yang dipakai bank dalam kewajiban mengganti kerugian adalah prinsip *strict liability* seperti yang dianut Pasal 19 ayat (1) UUPK, di mana pelaku usaha harus mengganti kerugian secara langsung tanpa membebankan pembuktian kepada konsumen bahwa pelaku usaha memang bersalah dan wajib mengganti rugi dan yang dapat membebaskan tanggung jawab tersebut hanyalah kelalaian konsumen sebagaimana diatur Pasal 27 huruf d UUPK.

Bentuk penggantian kerugian yang didapatkan nasabah belum diatur secara khusus oleh POJK PKJK, akan tetapi Pasal 19 ayat (2) UUPK telah mengatur bentuk ganti kerugian yang didapatkan nasabah. Yaitu dapat berupa pengembalian uang yang hilang.

Pasal 29 POJK PKJK sudah menjadi peraturan yang memenuhi kewajiban bank sebagai pelaku usaha untuk beritikad baik sebagaimana daitur Pasal 7 huruf a UUPK, karena POJK PKJK mewajibkan bank mengganti kerugian nasabah secara langsung ketika kerugian tersebut terjadi. Selain itu, POJK PKJK juga menjadi peraturan yang memenuhi kewajiban bank dalam pasal 7 huruf f UUPK yaitu memberi ganti rugi atas kerugian akibat penggunaan jasa misalnya layanan perbankan elektronik.

B. Analisis Penerapan Manajemen Risiko Layanan Perbankan Elektronik dan Prinsip Pertanggungjawaban Bank XYZ atas Kerugian Nasabah Akibat Penipuan *Sim Swap*

Dari hasil penelitian yang mengunakan sumber terbatas yaitu melalui penelusuran data tersier berupa laporan tahunan Bank XYZ tahun 2019. Maka penulis mendapat gambaran Bank XYZ menerapkan beberapa poin manajemen risiko layanan perbankan elektronik yang diatur oleh Pasal 2 ayat (2) POJK MRTI yaitu:

1. pengawasan aktif direksi dan dewan komisaris

Direksi Bank XYZ telah memenuhi unsur pengawasan aktif direksi sebagaimana diatur Pasal 5 POJK MRTI yaitu:

a. Direksi menetapkan rencana strategis teknologi informasi dan kebijakan bank terkait penggunaan teknologi informasi, Bank XYZ telah melaksanakan aturan tersebut karena direksi Bank XYZ terlihat pada bagian tugas dan tanggung jawab direksi juga tugas dan tanggungjawab komite pengarah teknologi informasi lapora tahunan bank XYZ tahun 2019 bahwa direksi dibantu komite pengarah teknologi informasi menetapkan rencana strategis teknologi infomrasi bank XYZ.
b. Direksi menetapkan kebijakan, standar, prosedur terkait penyelenggaraan teknologi informasi. Bank XYZ telah melaksanakan peraturan tersebut terlihat pada bagian tugas dan tanggung jawab komite pengarah teknologi informasi bahwa direksi dibantu oleh komite pengarah teknologi informasi

menyusun kebijakan, standar, dan prosedur penggunaan teknologi informasi yang utama.

c. Direksi memastikan terdapat kegiatan peningkatan kompetensi sumber daya manusia terkait penggunaan teknologi informasi. Bank XYZ telah melaksanakan hal ini melalui penyelenggaraan pelatihan dan pengembangan terhadap keterampilan teknis manajemen risiko dan teknologi informasi dalam bentuk pelatihan dan *workshop.*

Untuk dapat dikatakan bahwa bank telah memenuhi pengawasan aktif dewan komisaris, maka direksi Bank XYZ harus memenuhi unsur sesuai Pasal 6 POJK MRTI yaitu:

a. Mengevaluasi, mengarahkan, dan memantau Mengevaluasi, mengarahkan, dan memantau rencana strategis penggunaan teknologi informasi dan kebijakan bank terkait penggunaan teknologi informasi. Bank XYZ dalam hal ini telah melaksanakan ketentuan tersebut memberikan rekomendasi, saran, juga memantau dan mengevaluasi pelaksanaan kebijakan strategis Bank XYZ.
b. Mengevaluasi pertanggungjawaban direksi atas penerapan manajemen risiko dalam penggunaan teknologi informasi. Dalam hal ini Dewan Komisaris Bank XYZ telah melaksanakan hal tersebut dengan mengawasi kinerja direksi secara aktif mengenai segala tugas dan tanggung jawabnya.

Bank XYZ telah memiliki komite pengarah teknologi informasi sebagaimana diatur dalam Pasal 7 ayat (1) POJK MRTI dan berdasarkan asumsi atas analisis penulis, komite pengarah teknologi informasi Bank XYZ telah

melaksanakan tanggungjawab sebagaimana diatur dalam Pasal 7 ayat (2) POJK MRTI.

2. kecukupan kebijakan, standar, prosedur penggunaan teknologi informasi

Menurut penulis Bank XYZ telah melaksanakan amanah Pasal 8 ayat (1) dengan memiliki kebijakan, standar, dan prosedur penggunaan teknologi informasi yang disusun direksi dan dibantu oleh Komite Pengarah Teknologi Informasi. Akan tetapi penulis tidak menemukan secara khusus informasi mengenai kebijakan, standar dan prosedur layanan perbankan elektronik dalam laporan tahunan Bank.

Bank XYZ juga telah menerapkan limit risiko untuk seluruh jenis potensi risiko yang melekat dalam aktivitas bank sebagaimana diatur pasal 8 ayat (3) POJK MRTI.

3. kecukupan proses identifikasi, pengukuran, pemantauan, dan pengendalian risiko penggunaan teknologi informasi

Penulis tidak menemukan secara khusus mengenai pemantauan risiko layanan perbankan elektronik sebagaimana diatur SEOJK MRTI yaitu pembuatan pangkalan data yang berisi historis kerugian.

Penulis juga tidak menemukan secara lengkap mengenai proses pengendalian risiko layanan perbankan elektronik Bank XYZ sesuai yang diatur SEOJK MRTI, yang penulis temukan hanya Bank XYZ telah melakukan pengendalian menggunakan metode untuk menguji keaslian menggunakan

keamanan dua faktor (*two-factor authentication),* persyaratan jumlah *password* 6 (enam) kata, dan batas kesalahan memasukan *password* sebanyak tiga kali. Sedangkan penulis tidak menemukan informasi pengendalian risiko layanan perbankan elektronik yang lainnya sebagaimana diatur SEOJK MRTI dalam laporan tahunan Bank XYZ tahun 2019 maupun *website bank.*

4. sistem pengendalian intern atas penggunaan teknologi informasi.

   Bank XYZ telah melaksanakan sistem pengendalian intern teknologi informasi sebagaimana diatur Pasal 17 ayat (1) POJK MRTI :

   a. Pengawasan oleh manajemen dan adanya budaya pengendalian; Kegiatan pengendalian melibatkan seluruh jajaran Bank XYZ. Kegiatan pengendalian mencakup perencanaan, penetapan kebijakan dan prosedur, penerapan pengendalian serta proses verifikasi dini untuk memastikan bahwa kebijakan dan prosedur telah dipatuhi secara konsisten. Akan tetapi dalam faktanya, pengendalian tersebut menurut penulis dirasa kurang efektif berjalan disemua lini, karena masih adanya risiko kerugian yang diderita nasabah.
   b. Bank XYZ telah melaksanakan identifikasi dan penilaian risiko yang telah dijelaskan dalam proses manajemen risiko di atas.
   c. Kegiatan pengendalian dan pemisahan fungsi, Bank XYZ telah melaksanakan aturan ini dengan menerapkan sistem pengendalian intern dengan tiga lini akuntabilitas. Pegawai juga dilarang merangkap

jabatan di lingkungan internal Bank yang dapat menimbulkan benturan kepentingan *(conflict of interest).*

d. Sistem informasi, sistem akuntansi, dan sistem komunikasi. Bank XYZ dalam pelaksanaan sistem informasi untuk keperluan pemantauan profil dan transaksi Nasabah, telah memiliki sistem aplikasi untuk mengidentifikasi, menganalisa, memantau dan menyediakan laporan mengenai karakteristik transaksi yang dilakukan oleh Nasabah, termasuk identifikasi transaksi keuangan mencurigakan. Akan tetapi pada faktanya, pelaksanaan sistem informasi untuk memantau transaksi nasabah tidak berjalan dengan efektif karena tidak dapat mencegah timbulnya transaksi perbankan yang dilakukan oleh pihak ketiga akibat dari pembobolan sim swap.
e. Kegiatan pemantauan dan koreksi penyimpangan, yang dilakukan oleh satuan kerja operasional, satuan kerja audit intern maupun pihak lain. Bank XYZ telah memiliki satuan kerja audit intern (SKAI) untuk pemantauan dan koreksi penyimpangan.

Kasus pembobolan rekening melalui *mobile banking* dan *internet banking* yang terjadi kepada Ilham Bintang merupakan bentuk penipuan *sim swap* karena telah memenuhi unsur-unsur sebagai berikut:

1. Pelaku menggunakan surat kuasa palsu yang dilampiri fotocopy KTP nasabah. Pada kasus pembobolan rekening Ilham Bintang pelaku membuat KTP palsu untuk menggandakan *sim card* Indosat di gerai Indosat Bintaro Jaya Xchange.

2. Jika berhasil mendapatkan *sim card* pengganti, maka pelaku dapat mengirimkan dan menerima pesan singkat ke bank seakan-akan dia merupakan nasabah yang sesungguhnya. Pada kasus pembobolan rekening Ilham Bintang pelaku berhasil menggandakan *sim card* Indosat milik Ilham, pada saat ini pelaku dapat mereset *user id* dan *password* dari *mobile banking* dan *internet banking* milik Ilham Bintang.
3. Pelaku menghubungi *call center* bank, dan meminta bank untuk melakukan reset PIN, notifikasi perubahan PIN akan disampaikan ke *e-mail* maupun pesan singkat nasabah, di mana nomor ponsel nasabah sudah dikuasai pelaku. Pelaku pada kasus pembobolan rekening Ilham Bintang lalu mereset *password* akun *mobile banking* dan *internet banking* Ilham Bintang dengan menggunakan kode OTP *(one-time password)* yang dikirimkan ke nomor *sim card* yang telah dikuasai pelaku.
4. Jika pelaku telah mengetahui PIN *internet banking* maupun *mobil banking* nasabah, maka dapat digunakan untuk membobol rekening nasabah di bank. Pada kasus pembobolan rekening milik Ilham Bintang, pelaku melakukan 98 transaksi pada Bank XYZ dengan menggunakan akun *mobile banking* dan *internet banking* milik Ilham Bintang dengan total sebesar Rp. 200 juta.

Bank XYZ tidak mau mengganti kerugian kepada Ilham Bintang atas uangnya yang hilang sebesar Rp. 200 Juta yang diduga akibat penipuan sim swap dengan alasan bahwa *user id* dan *password* yang digunakan untuk masuk ke akun mobile banking dan internet banking milik Ilham Bintang telah benar dan Bank XYZ selalu mengirim OTP (*one-time password*) untuk konfirmasi

transaksi yang dilakukan sesuai dengan prosedur bank. Jadi, Bank XYZ merasa tidak memiliki kesalahan dalam kasus sim swap yang terjadi kepada Ilham Bintang dan Bank XYZ menolak mengganti kerugian.

Maka dari itu berdasarkan asumsi tersebut penulis menyimpulkan bahwa prinsip pertanggungjawaban yang dipakai Bank XYZ dalam kasus *sim swap* Ilham Bintang adalah prinsip praduga untuk selalu bertanggung jawab *(presumption of liability).* Hal ini bertantangan dengan prinsip pertanggungjawaban *strict liability* yang dianut Pasal 29 POJK PKJK.

Layanan perbankan elektronik Bank XYZ yang dapat dibobol melalui *sim swap* dan Bank XYZ tidak mengganti kerugian kepada nasabah akibat pembobolan tersebut dapat menimbulkan risiko reputasi yang mempengaruhi finansial perusahaan di mana nasabah dan masyarakat luas tidak mau lagi menyimpan uang di Bank XYZ.

Sebagaimana yang dikemukakan Hans Kelsen dalam jurnal *lex renaissance* pertanggungjawaban di atas merupakan bentuk tanggung jawab hukum, dalam kasus Ilham Bintang, bank memiliki kewajiban mengganti kerugian kepada nasabah berdasarkan Pasal 29 POJK PKJK yang apabila Bank tidak melaksanakan kewajiban tersebut akan menimbulkan sanksi dan konsekuensi hukum.

Berdasarkan asumsi saya bahwa Bank XYZ yang menolak memenuhi kewajibannya dalam hal ini mengganti kerugian nasabah akibat penipuan *sim swap*, seperti Bank XYZ yang menolak mengganti kerugian kepada Ilham Bintang, maka Otoritas Jasa Keuangan sebagai regulator industri perbankan

sudah seharusnya dapat memberikan sanksi administratif sesuai dengan ketentuan Pasal 53 POJK PKJK yaitu berupa:

a. Peringatan tertulis
b. Denda yaitu kewajiban untuk membayar sejumlah uang tertentu
c. Pembatasan kegiatan usaha
d. Pembekuan kegiatan usaha, dan
e. Pencabutan izin kegiatan usaha.